

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11)特許出願公表番号

特表平11-511882

(43)公表日 平成11年(1999)10月12日

(51) Int.Cl. ⁸		識別記号	F I		
G 0 6 F	15/00	3 3 0	G 0 6 F	15/00	3 3 0 F
	19/00		G 1 0 L	3/00	5 5 1 P
G 0 6 T	7/00		G 0 6 F	15/62	4 6 5 A
G 1 0 L	3/00	5 5 1		15/30	3 4 0
C					
			審査請求	未請求	予備審査請求 有

(全 202 頁)

(21)出願番号	特願平8-535098	(71)出願人	スマート タッチ, インコーポレイテッド
(86) (22)出願日	平成8年(1996)5月17日		アメリカ合衆国 カリフォルニア 94704,
(85)翻訳文提出日	平成9年(1997)11月17日		パークレー, シャタック スクエア 46,
(86)国際出願番号	PCT/US96/07185		スイート 12
(87)国際公開番号	WO96/36934	(72)発明者	ホフマン, ネット
(87)国際公開日	平成8年(1996)11月21日		アメリカ合衆国 カリフォルニア 94704,
(31)優先権主張番号	08/442, 895		パークレー, シャタック スクエア 46,
(32)優先日	1995年5月17日		スイート 12
(33)優先権主張国	米国(US)	(72)発明者	ベア, デイビッド エフ.
			アメリカ合衆国 カリフォルニア 94704,
			パークレー, シャタック スクエア 46,
			スイート 12
		(74)代理人	弁理士 山本 秀策

最終頁に続く

最終頁に続く

(54) 【発明の名称】 電子取引および電子送信の承認のためのトークンレス識別システム

(57) 【要約】

トランザクションおよび送信を承認するためのトークンレス識別システムおよび方法が開示される。本発明によるトークンレスシステムおよび方法は、主として、未知のユーザ本人から直接、収集された、指紋や声紋記録のようなユニークなバイオメトリックサンプルを、以前に得られ格納された同一タイプの認証済みバイオメトリックサンプルと相関的に比較することに基づいている。本発明は、その他の独立したコンピュータシステム間の完全な、または部分的な仲立ちとして作用するようにネットワーク化されうるし、あるいは、必要なすべての実行事項をおこなう単独のコンピュータシステムであってもよい。また、本発明は、識別が完了し、そのコンピュータシステムがアクセスされたことをユーザに認証し、示した後に、ユーザに返送されるプライベートコードの使用も考慮に入れている。さらに、本発明による識別システムおよび方法は、承認されたユーザが、アクセスの企ては強要されたものであることを機関に警告することを可能にする緊急通知手段をさらに備えている。

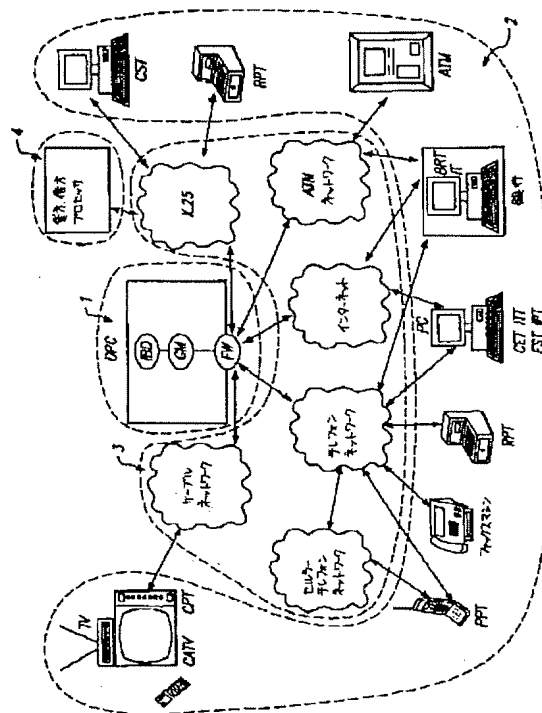


FIG. 1

【特許請求の範囲】

1. 送信権要求ステップの間に収集された少なくとも1つのバイオメトリックサンプルおよび個人識別コードの検査と、登録ステップの間に収集され、以前に記録されたバイオメトリックサンプルおよび個人識別コードとの比較とによって個人の同一性を判定する、自発的なトークンレス識別コンピュータシステムであって、

a. 少なくとも1つのコンピュータと、

b. 該登録ステップの間に、個人に、少なくとも1つのバイオメトリックサンプル、個人識別コード、およびプライベートコードを自発的に入力させる、第1の収集および表示手段であって、該プライベートコードが該個人により選択される、第1の収集および表示手段と、

c. 該送信権要求ステップの間に、個人に、少なくとも1つのバイオメトリックサンプルおよび個人識別コードを自発的に入力させる、第2の収集および表示手段と、

d. 該第1および該第2の収集および表示手段を該コンピュータに相互接続することによって、該収集されたバイオメトリックサンプル、該個人識別コードおよび該プライベートコードを該第1および該第2の収集手段から該コンピュータへと送信する、第1の相互接続手段と、

e. 該送信権要求ステップの間に収集された該バイオメトリックサンプルおよび該個人識別コードを、該登録ステップの間に収集された該バイオメトリックサンプルおよび該個人識別コードと比較することにより、評価を生じる手段と、

f. データを格納し、コマンドを処理、実行することによって、判定を生じる、該コンピュータ内の実行手段と、

g. 該コンピュータから該評価、該判定あるいは該プライベートコードを出力する手段と、

を備えた自発なトークンレス識別コンピュータシステム。

2. 前記第1および第2の収集および表示手段が、

a. ハードウェア部品およびソフトウェア部品をさらに有し、バイオメトリッ

クサンプルを収集する、少なくとも1つのバイオメトリック入力手段と、

b. 追加データを入力し、付加する、該バイオメトリック入力手段と機能的にその一部または全部が一体化された、少なくとも1つの端末手段と、

c. 個人識別コードを入力する少なくとも1つのデータ入力手段であって、該バイオメトリック入力手段または該端末手段のいずれか1つと一体化されている、データ入力手段と、

d. 該バイオメトリック入力手段、該データ入力手段および該端末を相互接続する、第2の相互接続手段と、

をさらに備えている、請求項1に記載の装置。

3. 前記バイオメトリック入力手段が、前記コンピュータに対して以前に登録されたハードウェア識別コードを有しており、該ハードウェア識別コードが、該バイオメトリック入力手段を該コンピュータにとって固有のものとして識別可能とする、請求項2に記載の装置。

4. 前記ハードウェア部品が、

a. データを処理する少なくとも1つのコンピューティングモジュールと、

b. データおよびソフトウェアを格納する消去可能メモリモジュールおよび非消去可能メモリモジュールと、

c. バイオメトリックデータを入力するバイオメトリックスキャナ装置と、

d. データを入力するデータ入力手段と、

e. デジタル通信ポートと、

f. 電子的盗聴を防止する手段と、

をさらに備えている、請求項2に記載の装置。

5. 前記ハードウェア部品が、無線通信手段をさらに備えている、請求項2に記載の装置。

6. 前記ソフトウェア部品がコンピューティングモジュール内に常駐しており、かつ

a. 少なくとも1つのコマンドインタフェースモジュールと、前記バイオメトリック入力装置の意図的使用のために特に構成された、第1セットのソフトウェ

アおよび関連づけられたデータと、データとが格納されている、電子的に消去可能なメモリモジュールと、

b. 第2セットのソフトウェアおよび関連づけられたデータが格納される、非消去可能なメモリモジュールと、

をさらに備えている、請求項2に記載の装置。

7. 前記ソフトウェア部品が、

a. 平文から暗号文へとデータを暗号化する手段と、

b. 少なくとも1つのデバイスドライバと、

をさらに備えている、請求項8に記載の装置。

8. 前記端末が、ファクシミリ機、電話、テレビジョンリモートコントロール、パーソナルコンピュータ、クレジット／デビットカードプロセッサ、キャッシュレジスタ、自動預金支払機および無線パーソナルコンピュータからなる群から選択される、請求項2に記載の装置。

9. 前記比較手段が、前記バイOMETリック入力手段を識別する手段をさらに備えている、請求項1に記載の装置。

10. 前記コンピュータシステムが、

a. 少なくとも1つの独立したコンピュータネットワークシステムと

b. 該コンピュータシステムを相手側のコンピュータシステムに相互接続する

第3の相互接続手段と、

をさらに備えている、請求項1に記載の装置。

11. 前記データベースが、個人バイOMETリックデータベースをさらに備えている、請求項13に記載の装置。

12. 個人を自発的にトークンなしに識別し、該識別を認証する方法であって、

a. 個人からの少なくとも1つのバイOMETリックサンプル、個人識別コードおよびプライベートコードが収集され、格納される、登録ステップと、

b. 個人からの少なくとも1つのバイOMETリックサンプルおよび個人識別コードが収集される、送信権要求ステップと、

c. 該送信権要求ステップの間に収集された該バイOMETリックサンプルおよ

び該個人識別コードが、該登録ステップの間に収集され格納された該バイオメトリックサンプルおよび該個人識別コードと比較されることにより、識別成功または識別失敗の結果を生じる、比較ステップと、

d. コマンドが処理され実行されることによって、判定を生じる、実行ステップと、

e. 該識別結果または該判定が外面化され、表示される、出力ステップと、

f. 該個人の識別に成功するとただちに、該プライベートコードが該識別されている該個人へと提示される、提示ステップと、を含む方法。

13. アカウントインデックスが緊急アカウントとしてラベルが付けられ、該アカウントがアクセスされた場合には、該緊急時が適切な機関に通知される、緊急アカウントインデックス割り当てステップをさらに含んでいる、請求項12に記載の方法。

14. 前記登録ステップおよび前記送信権要求ステップが、前記データを平文から暗号文へと変換する暗号化ステップをさらに含んでいる、請求項12に記載の方法。

15. 前記送信権要求ステップまたは前記登録ステップには、ユニークなハードウェア識別コードを有し、送信の度に1ずつ増加するシーケンスナンバをインクリメントする、ユニークな送信コードがさらに設けられている、請求項12に記載の方法。

16. 前記比較ステップが、反復送信を検出するのに前記ユニークな送信コードを使用することを含む、請求項12に記載の方法。

17. 前記比較ステップが、相手側の識別コードおよび前記ユニークな送信コードを用いる相手側識別ステップをさらに含む、請求項12に記載の方法。

18. 前記比較ステップが、前記送信権要求ステップの間に収集された前記個人の前記個人識別コードおよび前記バイオメトリックスを、前記登録ステップの間に収集された前記個人識別コードおよび前記バイオメトリックスと照合することにより、該個人を肯定的に識別することを含む、請求項12に記載の方法。

19. 前記実行ステップが、借受／貸付トランザクションステップをさらに含む、請求項12に記載の方法。

20. 前記実行ステップが、アーカイブ化ステップと、データをアーカイブするトラッキングコード割り当てステップとをさらに含む、請求項12に記載の方法。

21. 前記提示ステップが、前記プライベートコードを外面化することをさらに含む、請求項12に記載の方法。

22. 第1の個人からの少なくとも1つの以前に格納された第1のバイオメ

トリックサンプルを、個人識別コードバスケットを用いて迅速にサーチする方法において、該個人識別コードバスケットが、該個人識別コードバスケットにより識別される少なくとも1人の第2の個人からの少なくとも1つのアルゴリズム的にユニークな第2のバイオメトリックサンプルを含みうる、方法であって、

a. 格納ステップであって、

i. 該第1の個人による個人識別コードの選択と、

ii. 該第1の個人からのバイオメトリックサンプルの入力と、

iii. 該第1の個人により選択された該個人識別コードにより識別された該個人識別コードバスケットの位置を特定することと、

iv. 該第1の個人から取られた該バイオメトリックサンプルを、該選択された個人識別コードバスケット内に以前に格納されたバイオメトリックサンプルのいずれかと比較することにより、該第1の個人により入力された該バイオメトリックサンプルが、少なくとも1人の第2の個人により提供され、以前に格納された少なくとも1つのバイオメトリックサンプルと比べてアルゴリズム的にユニークであることを確かめることと、

v. もし該サンプルが、該少なくとも1人の第2の個人からの該少なくとも1つの以前に格納されたバイオメトリックサンプルと比べてアルゴリズム的にユニークであるのなら、該第1の個人からの該入力されたバイオメトリックサンプルを該選択された個人識別コードバスケットに格納することと、

を含む、格納ステップと、

b. 送信権要求ステップであって、

- i. 該第1の個人により該選択された個人識別コードを入力することと、
 - ii. 該第1の個人によりバイオメトリックサンプルを入力することと、
- を含む、送信権要求ステップと、
- c. 比較ステップであって、
 - i. 該第1の個人により入力された該個人識別コードにより識別される該個人識別コードバスケットを検索することと、
 - ii. 該第1の個人からの該入力されたバイオメトリックサンプルを、該入力された個人識別コードバスケットにおける該少なくとも1人の第2の個人からの該
- 少なくとも1つの格納されたバイオメトリックサンプルと比較することにより、識別成功または識別失敗のいずれかの結果を生じることと、
- をさらに含む、比較ステップと、
- を含む方法。

23. 送信権要求ステップの間に収集された少なくとも1つのバイオメトリックサンプルおよび個人識別コードの検査と、登録ステップの間に収集され以前に記録されたバイオメトリックサンプルおよび個人識別コードとの比較と、によって個人の同一性を判定する、自発的なトークンレス識別コンピュータシステムであって、

- a. 少なくとも1つのコンピュータと、
- b. 該登録ステップの間に、個人に、少なくとも1つのバイオメトリックサンプルおよび個人識別コードを自発的に入力させる、第1の収集および表示手段と、
- c. 該送信権要求ステップの間に、個人に、少なくとも1つのバイオメトリックサンプルおよび個人識別コードを自発的に入力させる、第2の収集および表示手段と、
- d. 該第1および該第2の収集および表示手段を該コンピュータに相互接続することによって、該収集されたバイオメトリックサンプルおよび該個人識別コードを該第1および該第2の収集手段から該コンピュータへと送信する、第1の相互接続手段と、

e. 該送信権要求ステップの間に収集された該バイオメトリックサンプルおよび該個人識別コードを、該登録ステップの間に収集された該バイオメトリックサンプルおよび該個人識別コードと比較することにより、評価を生じる手段と、

f. データを格納し、コマンドを処理、実行することによって、判定を生じる、該コンピュータ内の実行手段と、

g. 該コンピュータから該評価または該判定を出力する手段と、
を備えた自発的なトークンレス識別コンピュータシステム。

24. 前記第1および第2の収集および表示手段が、

a. ハードウェア部品およびソフトウェア部品をさらに有し、バイオメトリックサンプルを収集する、少なくとも1つのバイオメトリック入力手段と、

b. 追加データを入力し、付加する、該バイオメトリック入力手段と機能的にその一部または全部が一体化された、少なくとも1つの端末手段と、

c. 個人識別コードを入力する少なくとも1つのデータ入力手段であって、該バイオメトリック入力手段または該端末手段のいずれか1つと一体化されている、データ入力手段と、

d. 該バイオメトリック入力手段、該データ入力手段および該端末を相互接続する、第2の相互接続手段と、
をさらに備えている、請求項23に記載の装置。

25. 前記バイオメトリック入力手段が、前記コンピュータに対して以前に登録されたハードウェア識別コードを有しており、該ハードウェア識別コードが、該バイオメトリック入力手段を該コンピュータにとって固有のものとして識別可能とする、請求項24に記載の装置。

26. 前記ハードウェア部品が、

a. データを処理する少なくとも1つのコンピューティングモジュールと、

b. データおよびソフトウェアを格納する消去可能メモリモジュールおよび非消去可能メモリモジュールと、

c. バイオメトリックデータを入力するバイオメトリックスキャナ装置と、

d. データを入力するデータ入力手段と、

e. デジタル通信ポートと、
f. 電子盗聴を防止する手段と、
を備えている、請求項24に記載の装置。

27. 前記ハードウェア部品が、無線通信手段をさらに備えている、請求項24に記載の装置。

28. 前記ソフトウェア部品がコンピューティングモジュール内に常駐しており、かつ

a. 少なくとも1つのコマンドインタフェースモジュールと、前記バイオメトリック入力装置の意図的使用のために特に構成された、第1セットのソフトウェアおよび関連づけられたデータと、データとが格納されている、電子的に消去可能なメモリモジュールと、

b. 第2セットのソフトウェアおよび関連づけられたデータが格納される、非消去可能なメモリモジュールと、
をさらに備えている、請求項24に記載の装置。

29. 前記相互接続手段が、無線通信用の手段である、請求項24に記載の装置。

30. 前記比較手段が、前記バイオメトリック入力装置を識別する手段をさらに備えている、請求項23に記載の装置。

31. 前記コンピュータシステムが、

a. 少なくとも1つの相手側コンピュータシステムと、
b. 該コンピュータシステムを該相手側コンピュータシステムに相互接続する第3の相互接続手段と、
をさらに備えている、請求項23に記載の装置。

32. 個人を自発的にトークンなしに識別し、該識別を認証する方法であって、

a. 個人からの少なくとも1つのバイオメトリックサンプルおよび個人識別コードが収集され、格納される、登録ステップと、

b. 個人からの少なくとも1つのバイオメトリックサンプルおよび個人識別コードが収集される、送信権要求ステップと、

c. 該送信権要求ステップの間に収集された該バイオメトリックサンプルおよ

び該個人識別コードが、該登録ステップの間に収集され格納された該バイオメトリックサンプルおよび該個人識別コードと比較されることにより、識別成功または

は識別失敗の結果を生じる、比較ステップと、

d. コマンドが処理され実行されることによって、判定を生じる、実行ステップと、

e. 該識別結果または該判定が外面化され表示される、出力ステップと、を含む方法。

33. アカウントインデックスが緊急アカウントとしてラベルが付けられ、該アカウントがアクセスされた場合には、該緊急時が適切な機関に通知される、緊急アカウントインデックス割り当てステップをさらに含んでいる、請求項32に記載の方法。

34. 前記登録ステップおよび前記送信権要求ステップが共に、データの改変を検出する能力を提供するデータ隠蔽ステップをさらに含んでおり、

a. 秘密鍵と、

b. 該秘密鍵なしには再生されえない該データの非可逆的一方向変換と、を含む、請求項32に記載の方法。

35. 前記比較ステップが、反復送信を検出するのに前記ユニークな送信コードを使用することをさらに含む、請求項32に記載の方法。

36. 前記比較ステップが、前記送信権要求ステップの間に収集された前記個人の前記個人識別コードおよび前記バイオメトリックスを、前記登録ステップの間に収集された前記個人識別コードおよび前記バイオメトリックスと照合することにより、該個人を肯定的に識別することを含む、請求項32に記載の方法。

【発明の詳細な説明】**電子取引および電子送信の承認のためのトークンレス識別システム****背景**

今日の金融界ではトークンおよびクレジットカードの使用が広く普及している。トークンは何らかの無生物であり、これを提示する個人に、権限をあたえるものである。金融口座への遠隔アクセスはすべてトークンまたはプラスチックカードを用いて行われる。デビットカード（debit card）で食品雑貨を購入する場合も、クレジットカードで消費財を購入する場合も、その取引の中心にあるのは、個人と、個人がアクセスしている金融口座とを識別する役割を果たすクレジットカードまたは「スマートカード（smart card）」などのトークンによって可能となる金銭の移動である。残念なことに、この便利なトークンベースの金銭移動システムと組み合わせた現在の技術で得られたシステムは、盗みおよび詐欺が起こりやすいシステムである。

ユーザ同一性の検証は、個人間で容易に再生できかつやりとりできるトークンにあるデータのみに基づいて行われ、そのような場合の安全性は、承認されたユーザおよびマーチャントがこの情報を所有物として維持する際の努力と運とをあてにしなければならないものである。しかし、トークンは、その本質により、個人とあまり強い関連があるわけではない。トークンの正当な所有者の識別はどうみても十分ではない。このことは、トークンの正当な所有者以外の個人がこれらのトークンを用いてマーチャントおよび他の消費財供給者に詐欺行為をはたっていることから容易に証明される。

このシステムがその性質上非常に無防備であるため、クレジット業界では多くの様々な地域で詐欺による損害が起こっているが、この損害は主に、紛失したカード、盗まれたカード、あるいは偽造カードによるものである。クレジットカードは個人識別コード（personal identification code）（PIC）を使用しなければ使えないため、紛失カードが他人の手に渡った場合、カードを現金に換えることができる。システムの詐欺の大部分がトークンを盗むことにより起こっているため、偽造クレジットカードの使用が増加し続けている。クレジットカードは

より高度な技術を持つ者によって偽造されており、カード保有者の有効な口座番号を得て、この有効な番号を用いて偽造カードを作っている。偽造者は、磁気ストリップを符号化し、偽造プラスチックカードに口座番号を打ち出す（emboss）。このカードをマーチャントに提示すると、正当なカード保有者の口座に支払いが請求される。他の形態の損害は、マーチャントがカード保有者の口座番号を不正に利用するという犯罪行為によって起こる損害である。さらに、承認されたカード保有者がトークンを用いて買い物をし、その後にトークンを紛失したあるいは盗まれたとして申請するというタイプの詐欺もある。すべてのタイプの詐欺による損害は年間9億5000万ドルを越えると推定される。

一般に、デビットカードは個人識別コード（P I C）とともに用いられる。デビットカードの偽造は、口座番号だけではなくP I Cも知る必要があり、それを知って初めてカードを作ることができるため、クレジットカードの場合よりも困難である。しかし、様々な戦略を用いて、不注意なカード保有者からP I Cを得ており、この戦略には、ショッピングモールにあり、現金を分配するがP I Cを記録するトロイの木馬のように危険な現金自動預け払い機（automated teller machine）すなわちA T Mから、これもP I Cを記録するマーチャント用販売時点情報管理（P O S）デバイス、およびカード保有者がA T MでP I Cを入力するのを双眼鏡で見る人といったものがある。その後に偽造したデビットカードを様々なA T M機で用いてその不運な口座が空になるまで使うのである。

この偽造詐欺のため、産業界では、過去10年間にわたって、クレジットカード取引システムの使用については根本的な変更はせずにトークンを変更した。この対処法は、顧客に自分のカードをアクティベートするように発行者に依頼してもらうといった主に管理上の変更であった。他の変更としては、ホログラム、写真I D、または改良を加えた署名領域の追加がある。これらのタイプの変更は特に、システムで個人の真の識別がなされていないために詐欺が容易であることを示している。これらの変更を行えば、製造コストが年間20億ドルに倍増すると推定される。

銀行業界は、近い将来、「スマートカード」と呼ばれるさらに高価なカードに

移行するであろうと予測している。スマートカードは、最初のホームコンピュータのうちの幾つかのものが持っていた計算力と同等の計算力を含む。第1世代のスマートカードの現在のコスト見積は、流通コストを除いて約3.50ドルであると推定され、これは、プラスチックカードブランクの0.30ドルよりもかなり高い。

電子金融取引の普及に加えて、およびその普及に伴って、現在では、電子ファクシミリ、電子メールメッセージおよび同様の電子通信が広く用いられている。個人が適切に識別されないという金融取引に関する問題点と同様に、電子送信に関しても個人が適切に識別されないという問題点がある。電子通信は、その簡便さおよび速度ならびに従来の郵便よりも低いコストによって、似通った個人およびビジネス間におけるえり抜きの通信方法となった。しかし、ファクシミリおよび電子メール（または、「Eメール」もしくは「eメール」）などの非常に多くの電子メッセージの場合、それを送ってもそれが真の宛先に届いているかどうか、または特定の個人が実際にその電子メッセージを送信もしくは受信したかどうかは分からない。さらに、電子メッセージを送信または受信した個人の識別名（identify）を確かめる方法がない。

以上のことに鑑みて、詐欺が非常に起こりにくく、実用的で、ユーザが迅速に電子取引および電子伝送を操作しかつ実行するのに効率的なコンピュータアクセスシステムが長い間必要とされている。

個人が個人間で自由にやりとりできる何らかの物理的なものを所有しているかどうかを検証するのではなく、承認されたユーザに固有で身体的に個人的なものであるバイオメトリクスと、個人識別コードとのみに基づいてユーザの個人識別名を検証することができるコンピュータシステムも必要とされている。

特に、多数のまたは厄介なコードを覚える必要性を大幅に少なくするまたはなくし、アクセスリクエストを開始するために所有者の財産物（proprietary object）を所有し、携帯し、提示する必要性をなくす金融取引システムが必要とされている。

さらに、ユーザが、多数の口座にアクセスし、ユーザに対して承認されたすべてのサービスを獲得し、すべての金融口座における取引およびすべての金融口座

間の取引を行い、購入品の支払いを忘れずに行い、様々なサービスを受けることができるようにするコンピュータシステムも要求されている。

さらに、このコンピュータシステムは、様々な電子取引デバイス、電子送信デバイス、およびシステム構成を有する既存のネットワークと動作的に互換性があるほど十分に柔軟で、手頃なものでなければならない。

最後に、電子メールメッセージおよび電子ファクシミリが安全に送信および受信され、電子メッセージの内容が承認されていない個人に漏れないように保護され、送り手または受け手の識別名を高い確実性で得ることができるようにする必要がある。

発明の要旨

本発明は、送信権要求ステップの間に収集された個人のバイオメトリックサンプルおよび個人識別コードを、その個人について、登録ステップの間に収集され、データ処理センターのある遠隔サイトに格納されたバイオメトリックスサンプルおよび個人識別コードと比較することによって個人の同一性を判定する、改善された識別システムを提供することによって、これらの要求を満たす。本発明は、入力されたバイオメトリックサンプルおよび個人識別コードを比較する手段を備え、さまざまなデータベースおよびメモリモジュールを備えた、コンピュータネットワークホストシステムを備えている。また、本発明は、バイオメトリックスおよび個人識別コード入力装置と、いったん個人の同一性が判定された後、要求されたトランザクションおよび送信をホストシステムにより実行する情報を提供するためのデータ入力端末と、を備えている。また、本発明は、ホストシステムを、端末およびバイオメトリックス入力装置に接続する手段をも備えている。

コンピュータは、また、従来のデータ格納および変更と共に、さまざまなトランザクションおよび送信を実行する手段も備えている。さらに、コンピュータは、バイオメトリックス—P I C（「個人識別コード」）の比較の評価、およびトランザクションまたは送信の何らかの実行について、識別評価またはステータスの判定を出力することができる。また、コンピュータシステムは、登録ステップの間に個人により以前に選択された秘密コードをその個人に返送することによって、

そのコンピュータシステムがアクセスされたことを、現在、識別されている個人に通知し、そのことを認証する。

好ましくは、このコンピュータシステムは、電子的盗聴および電子的侵入およびウイルスから保護される。バイオメトリックサンプルおよび個人識別コードを収集するためにこのコンピュータにより用いられる装置は、a) ハードウェア部品およびソフトウェア部品を有し、バイオメトリックサンプルを収集する、少なくとも1つのバイオメトリック入力装置と、b) 補助データを入力し、付加する、バイオメトリック入力手段と機能的にその一部または全部が一体化された、少なくとも1つの端末装置と、c) 個人識別コードを入力する少なくとも1つのデータ入力装置であって、バイオメトリック入力装置または端末装置のいずれか1つと一体化されている、データ入力装置と、d) バイオメトリック入力装置、データ入力装置および端末を相互接続する手段と、を備えている。この端末装置は、また、データおよび情報を表示する少なくとも1つの表示装置を備えている。さらなるセキュリティを保証するために、このコンピュータシステムは、バイオメトリック入力装置を固有のものとして識別し、バイオメトリック入力装置に接続されている端末に関わる相手側の識別コードすなわちマーチャント識別コードを通して、相手側すなわちマーチャントを固有のものとして識別する。また、好ましくは、このバイオメトリック入力装置は物理的および電子的改変から保護されており、この装置が物理的に侵害された場合には、その装置内の部品を物理的および／または電子的に破壊し、および／または装置のメモリモジュールから重要なデータを消去する手段が用いられる。

加えて、このバイオメトリック入力装置は、データ処理モジュールと、データおよびソフトウェアを格納する消去可能メモリモジュールおよび非消去可能メモリモジュールと、バイオメトリックデータを入力するバイオメトリックスキャナ装置と、データを入力するデータ入力装置と、デジタル通信ポートと、を備えたハードウェア部品を備えている。

バイオメトリック入力装置、端末およびコンピュータネットワーク間で送られた電子的データの完全性および秘匿性を保護するためには、このデータは暗号化され、シールされるのが好ましい。

ホストコンピュータシステムは、また、その他の独立したコンピュータシステム、データベース、ファクシミリ機、およびその他のネットワークと、従来の手段を介して接続されており、それらと通信することができる。

本発明の方法は、個人により提供された少なくとも1つのバイオメトリックサンプルと、やはりその個人により提供された個人識別コードとを検査することにより、トークンを全く用いず、自発的に個人を識別することを含む。登録ステップにおいて、個人は、システムに対して、認証されたバイオメトリックサンプルと、個人識別コードと、秘密コードとを登録することが求められる。その後、送信権要求ステップにおいて、この個人のバイオメトリックスサンプルおよび個人識別コードが収集され、登録ステップの間に登録されたものと比較される。個人識別コードおよびバイオメトリックスサンプルが一致すると、その個人が肯定的に識別される。現実のコンピュータシステムにアクセスされたことを識別された個人に認証するために、登録ステップにおいて集められた個人の秘密コードは、個人に返送される。

本発明の方法は、好ましくは、登録の間にバイオメトリックスサンプルを検査し、以前に悪事を企てたとして指定されている個人、または実際に詐欺によりシステムに悪事を働いた個人から集められたバイオメトリックスサンプルと、そのようなバイオメトリックスサンプルとを比較する方法を含む。

好ましい実施の形態では、本発明は、緊急状況の存在、または承認されたユーザが脅迫されていることを機関に通知する方法を含む。

また、ファクシミリまたは電子メールメッセージのような何らかの文書が、その文書を将来識別するためのアルゴリズムを用いて、固有のものとしてチェックサムされるのも好ましい。

本発明のさらに別の方法は、異なる複数の個人からのいくつかの類似していないバイオメトリックスサンプルを、ある個人識別コードにより識別される電子バスケットに格納し、個人のバイオメトリックスサンプルおよび個人識別コードを検査することによって、その個人を迅速に識別することができる。

本発明のある実施の形態では、コンピュータシステムは、各個人が、遠隔データ処理センターにより選択された1グループの個人識別コード（「PIC」）か

ら

自らのP I Cを選択することを可能にする。これは、いったん個人のバイオメトリックが収集されると、データ処理センターが、記憶するにふさわしい (conductive to) いくつかのP I Cをランダムに選択する方法においておこなわれる。その後、データ処理センターは、収集されたこれらのバイオメトリックと、P I Cバスケットまたはグループに既に存在しているバイオメトリックとの比較をおこなう。新規登録者のバイオメトリックが、これらのランダムに選択されたP I Cグループのいずれか1つに対して割り当てられ、以前に登録されたバイオメトリックと類似している場合には、そのP I Cは、新しい個人により使用されるデータベースにより拒絶され、別のそのようなバイオメトリック比較をおこなうために、代替りのP I Cが選択される。いったんデータ処理センターが、いくつかの類似したバイオメトリックスを混同することなく、いくつかのP I Cオプションを発生した後、これらのP I Cは、新規登録者に提示され、個人は、そこから1つのP I Cを選択することができる。

本発明のある実施の形態では、第1の個人からの少なくとも1つの以前に格納された第1のバイオメトリックサンプルを、個人識別コードバスケットを用いて迅速にサーチする方法において、個人識別コードバスケットが、上記個人識別コードバスケットにより識別される少なくとも1人の第2の個人からの少なくとも1つのアルゴリズム的にユニークな第2のバイオメトリックサンプルを含みうる、方法が提供される。この方法は、まず、格納ステップであって、a) 第1の個人による秘密コードの選択と、b) 上記第1の個人による個人識別コードの選択と、c) 上記第1の個人からのバイオメトリックサンプルの入力と、d) 上記第1の個人により選択された個人識別コードにより識別された個人識別コードバスケットの位置を特定することと、e) 上記第1の個人から取られたバイオメトリックサンプルを、上記選択された個人識別コードバスケット内に以前に格納されたバイオメトリックサンプルのいずれかと比較することにより、上記第1の個人により入力されたバイオメトリックサンプルが、少なくとも1人の第2の個人により提供され、以前に格納された少なくとも1つのバイオメトリックサンプルと

比べてアルゴリズム的にユニークであることを確かめることと、f) もし上記サンプルが、上記少なくとも1人の第2の個人からの上記少なくとも1つの以前に格納

されたバイオメトリックサンプルと比べてアルゴリズム的にユニークであるのなら、上記第1の個人からの入力されたバイオメトリックサンプルを選択された個人識別コードバスケットに格納することと、を含む、格納ステップを含む。また、送信権要求ステップであって、a) 上記第1の個人により上記選択された個人識別コードを入力することと、b) 上記第1の個人によりバイオメトリックサンプルを入力することと、を含む、送信権要求ステップをも含む。さらには、比較ステップであって、a) 上記第1の個人により入力された上記個人識別コードにより識別される個人識別コードバスケットを検索することと、b) 上記第1の個人からの入力されたバイオメトリックサンプルを、上記入力された個人識別コードバスケットにおける上記少なくとも1人の第2の個人からの上記少なくとも1つの格納されたバイオメトリックサンプルと比較することにより、識別成功または識別失敗のいずれかの結果を生じることと、を含む、比較ステップをも含む。また、a) コマンドが処理され実行されることによって、判定を生じる、実行ステップと、b) 上記識別結果または上記判定が外面化され表示される、出力ステップと、c) 上記第1の個人の識別に成功するとただちに、上記秘密コードが上記第1の個人へと提示される、提示ステップと、をも含む。

本発明のある実施の形態によれば、ホストシステムは、識別されている個人と、アクセスされるべき別のコンピュータネットワークとの間に直列に位置づけられることによって、インタフェースとして作用する。なお、この実施の形態において、ユーザは、VISANTのような他の独立し安全の保証されたコンピュータシステムと動作的にインタラクティブである、本発明によるホストコンピュータシステムへと直接、アクセスリクエストを提出することは理解されたい。よって、このコンピュータシステムは、それがサービスする安全の保証されたコンピュータシステムそれぞれのすべての承認済みユーザについて認証されたバイオメトリックデータサンプルを維持する。これらのデータは、承認済みユーザ各人

により相互参照される。よって、同一性の検証が終了した後、セキュリティシステムは、ユーザに対して、ユーザがアクセスを承認されているシステムのリストを提供し、ユーザに対して所望のネットワークを選択するようプロンプトする。その後、リクエストされた実行ステップおよびトランザクションに関する情報は、今日、マ

ーチャントとクレジットカード会社との間でやりとりされている通信と似たタイプの選択された独立コンピュータネットワークへと送出される。

第2の実施の形態では、ホストシステムは、また、例えば、金融アカウントから借り受けたり、そこへ貸し付けたりすることのような、その他の独立したコンピュータシステムの機能を実行することもできる。このシステムでは、本発明のコンピュータシステムは、外部の独立したコンピュータネットワークを用いずに、個人によりリクエストされた機能を実行する。

本発明によるさらに別の実施の形態によれば、ホストコンピュータシステムへのアクセスをリクエストするサードパーティによりユーザが強要されているアクセスの企ての間に、予め指定された機関へと警告を発する手段が提供される。このような実施の形態では、承認されたユーザは、いくつかのコードをもつことになる。これらのコードの大半は、コンピュータシステムにより標準的アクセスコードとして認識されることになるが、他のものは、緊急コードとして認識されることになる。本発明のコンピュータシステムの比較手段は、承認されたユーザ1人につき少なくとも1つのコードを受け入れ、認識するように構成されており、ユーザにより入力されたコードが緊急コードと一致する時にはいつでも、緊急警告手段を作動させるように構成される。同時に、ユーザについて承認済みの同一性が判定されると、おそらくは制約されるように予め定められたアクセスレベル、またおそらくはミスリーディングデータ（すなわち「偽の画面」）が表示される結果となるアクセスレベルにおいて、リクエストされた安全の保証されたコンピュータシステムへのアクセスがそのユーザに許される結果となる。これにより、ユーザにより緊急通知が入力されたことを、強要者のサードパーティが知るのを防止できる。緊急コードは、ユーザの個人識別コードの一部として、あるいは

それと同時に入力されるか、またはコンピュータシステムへのアクセス時に緊急アカウントインデックスを選択することによって入力される。いずれの場合にせよ、アクセスをリクエストするユーザの利益は、もしそのユーザが機関への通知を企てていたことを強要者であるサードパーティが知ったのなら、危険にさらされることになる。

本発明は、いくつかの点で、明らかに従来技術よりもすぐれている。第1に、

ユーザにとって、特にユーザが金融アカウントにアクセスしようとしている時には、本発明は、きわめて簡単で、効率がよい。なぜなら、人は、アカウントにアクセスするのに、トークンをもっていることも提示することも必要なくなるからである。本発明は、要求された何らかのトークンを携帯し、安全保護し、その在処を突き止めることに関わるあらゆる不便をなくす。また、トークンは、特定のトークンに割り当てられた秘密コードを覚えていることをさらに要求する特定のコンピュータシステムに固有であることがよくあるので、本発明は、そのようなトークンを一切排除し、ただ1つの個人識別コードを用いてすべての資産へのアクセスを実現することによって、消費者にますます要求されている記憶および義務履行の量を大幅に減らすことができる。よって、一回限りのトークンレストランザクションで、消費者は、銀行アカウントからの現金の引き出しから、契約条項へと同意することを認めること、テレビジョンから直接、購入すること、さらには固定資産税の支払いに至るまで、ほとんどありとあらゆる商業的やりとりまたは電子的メッセージのやりとりを効率よく、かつ安全に実行することができる。

このような電子トランザクションは、また、操作コストを大幅に削減することによって、マーチャントおよび銀行が、大量の時間および出費を節約することを可能にする。本発明のシステムは、消費者が自らのもつ金融アカウントのすべてに対して同時に直接、アクセスすることを可能にするように設計されているので、金銭、小切手、商業書類その他を伴うトランザクションの必要性は大幅に低くなり、それにより、このようなトランザクション用の設備コストおよび収集・計算に必要なスタッフを減らすことができる。また、クレジットカード、ATMカ

ード、名刺などを発行し、再発行するための実質的な製造コストおよび配布コストをなくすることができるので、マーチャント、銀行ひいては消費者にとってさらに経済的な節約が可能になる。

本発明は、ユーザの1つ以上のユニークなバイオメトリックス特徴の分析に基づきユーザの同一性を判定することによって、非承認ユーザにアクセス権を賦与する危険性を実質的に排除することができる。

また、本発明は、認証データを維持し、ユーザのリクエストしているアクセスからは操作的に分離されたシステムにおける一点で同一性検証操作を実行するこ

とによって、詐欺に対する抵抗力をさらに強化し、それにより、ユーザが、認証データのコピーを取ったり、検証プロセスを改変したりするのを防止することができる。このようなシステムは、例えば、パーソナルコードのような認証情報がトークンに基づいて格納され、トークンから復元されうることになっており、かつ実際の同一性判定が、アクセスプロセス中にユーザと操作を通じてコンタクトを取っておこなわれる可能性のある、現存のトークンに基づくシステムよりも明らかに優れている。

よって、本発明の目的は、システムアクセスリクエストを開始するに当たって、ユーザが、例えばトークンのような物理的オブジェクトを所有し、提示する必要があるようにするコンピュータアクセス識別システムを提供することにある。

本発明の別の目的は、所有物および所有情報の所有を検証するのではなく、ユーザの同一性を検証できるコンピュータアクセス識別システムを提供することにある。

本発明のさらに別の目的は、ユーザにとって物理的に個人独特のものである1つ以上のユニークな特性に基づいて、ユーザの同一性を検証することにある。

ユーザにより提供された所望のコンフィギュレーションに従って、コンピュータシステム上でユーザのトランザクション能力を自動的に制約するコンピュータアクセス識別システムもまた必要とされている。本発明の上記利点およびその他の利点は、添付の図面と併せて、以下に述べる本発明の詳細な説明を読めば、さらに明らかになるであろう。

図面の簡単な説明

図1は、本発明のシステムの図である。

図2は、データプロセッシングセンター（DPC）およびその内部データベースおよび実行モジュールの図である。

図3は、小売POSターミナル、バイオメトリックス入力装置およびその構成要素、およびそれらの間の相互接続の図である。

図4は、リクエストパケットを生成するための、バイオメトリックス入力装置およびターミナルの動作のフローチャートである。

図5は、リクエストパケットおよびそれが包含する必須およびオプションデータを描写した図である。

図6は、レスポンスパケットおよびそれが包含する必須およびオプションデータを描写した図である。

図7は、バイオメトリックス入力デバイスにおける、データ暗号化およびシーリングプロセスを表すフローチャートである。

図8は、DPCにおけるデータ復号化およびカウンタパーティ識別プロセスを表すフローチャートである。

図9は、DPCにおけるデータ暗号化およびシーリングプロセスを表すフローチャートである。

図10は、登録プロセス中の個人の登録を表すフローチャートである。

図11は、個人の識別および個人ヘブライベートコードを返すプロセスを示すフローチャートである。

図12は、DPCおよびある実行ステップで起こるプロセスの概略のフローチャートである。

図13は、DPCにおける緊急リクエストおよびレスポンスプロセスのフローチャートである。

図14は、DPCにおける小売トランザクション承認実行動作の全体のフローチャートである。

図15は、DPCにおける遠隔トランザクション承認実行動作の全体のフローチャートである。

ャートである。

図16は、DPCにおけるATMアカウントアクセス実行動作の全体のフローチャートである。

図17は、DPCにおける発行者バッチ改変実行動作の全体のフローチャートである。

図18は、DPCにおける安全なファックス入力および電子文書入力実行動作の全体のフローチャートである。

図19は、DPCにおける安全なファックスデータおよび電子文書データ実行動作の全体のフローチャートである。

図20Aは、電子署名リクエストパケットを描写した図である。

図20Bは、電子署名レスポンスパケットを描写した図である。

図20Cは、電子署名検証リクエストパケットを描写した図である。

図20Dは、電子署名検証リクエストパケットを描写した図である。

図21は、DPCにおける電子署名実行動作の全体のフローチャートである。

図22は、DPCにおける電子署名検証実行動作の全体のフローチャートである。

発明の詳細な説明

このように、本発明の主な目的は、金融取引および金融以外の伝送を行うことを目的とした、個人を識別するための、多くのユーザーに対応できる、トークンレス装置および方法を提供することである。消費者が、いかなるトークン、クレジットカード、バッジ、あるいは運転免許証を含む身分証明書を使用することなく、これらの取引を遂行することができる、ということが、本発明の本質である。システムは、複数の銀行やクレジットアカウント (credit accounts) から、クレジットカードによる購入やATMサービスのような金融取引を完了するのに必要な速度で動作する。本システムは安全であるので、個人の記録およびバイオメトリックス情報は、個人を識別し、取引を承認するコンピューターシステム内においても、またコンピューターシステムとそのコンピューターシステムが通信する遠隔地との間のデータ転送中においても、機密かつ安全なままである。さらに

、このシステムは、識別および承認における誤りが、システムの使用を阻害したり、扱いにくくしたりしてはいけないという点において、信頼性がある。個人の識別には、バイオメトリックスの使用のみが想定されているので、システムには、緊急の場合には、承認されたユーザーに対してでさえ、アクセスを削減したり、当局（authorities）に通報したりする安全対策が講じられている。

ここで図を見ることにする。本発明の全体的な構成およびその構成要素が図1に示されている。基本的に、データプロセッシングセンター（DPC）1は、いくつかのタイプの内の1つであり得る、様々なタイプの通信手段3によって、様々なターミナル2に接続されている。DPCはまた、独立したコンピュータネットワーク4に接続され、これと通信する。DPCは、図2に示すように、いくつか

のデータベースおよびソフトウェア実行モジュールを含む。発明の好適な実施形態では、データベースは、安全保護のため、バックアップされるか「ミラーリング」されている。ファイアウォールマシン5はシステムの電子的侵入を防止する役割を果たしているのに対し、ゲートウェイマシン6は全データベースの追加、削除およびその他の改変を含む、ユーザーからのすべてのリクエストを実行する役割を果たしている。ゲートウェイマシンはまた、MACMモジュール7、MDMモジュール8、およびSNMモジュール9を用いたターミナルから届いたデータを復号およびデパッケージ（de-packaging）する役割も果たす。PGLモジュール10およびIMLモジュール11は、適切な個人識別コードおよびバイオメトリックスサンプルバスケットを見つけるために使用される。図3はターミナルおよびバイオメトリックススキャナー13、キーパッドあるいはPINパッド14のようなデータ入力手段および表示パネル15を有するバイオメトリックス入力デバイス12の一例を示している。バイオメトリックススキャナーは、指紋スキャナー、音声認識、掌紋スキャナー、網膜スキャナー等のいずれでもあり得るが、指紋スキャナーを例として使用する。バイオメトリックス入力デバイスはさらに、コンピューティングモジュール16、デバイスドライバ、および消去可能および消去不可能メモリモジュールを備えている。バイオメトリックス入力デバイスは、好適にはシリアルポート17を通してターミナルと通信する。ターミナ

ル2は、従来のモデム18、リクエストパケット19およびレスポンスパケット20を通し、ケーブルネットワーク、セルラー電話ネットワーク、電話ネットワーク、インターネット、ATMネットワーク、あるいはX.25のような、図1の相互接続手段の1つを用いてDPC1と通信する。図4は、リクエストパケット19およびバイオメトリックス入力デバイスソフトウェアによるその生成方法を描写した図である。図5および図6は、オプションおよび必須のデータセグメントを有するリクエストパケットおよびレスポンスパケットを描写した図である。さらに、パケットのどの部分が暗号化されており、どの部分がシールされているかも示されている。図7は、データの暗号化およびシーリングの全体的なプロセスのブロック図であり、メッセージ認証コードキー(MAC)21を用いたリクエストパケットシーリング前の、追加データ付加前の、データ暗号化用のD

UKPTキーデータ20の使用を示している。図8および図9は、DPCでの復号化および暗号化プロセスを示している。図12から19および21から22は、DPCで続行される実行ステップの選択例のブロック図である。

図面、図、フローチャートの説明、およびハードウェア構成要素、ソフトウェア構成要素、実行モジュール、データベース、接続手段、それらの間で転送されたデータを含む本発明の説明、および本発明の方法の説明を、以下で詳細に行う。

バイオメトリック入力装置(BIA)

BIAは、個人の識別に使用するためのバイオメトリック入力を収集、コード化および暗号化することをそのジョブとするハードウェアおよびソフトウェアの組み合わせである。BIAのすべてのアクションは、ターミナルと呼ばれる外部の制御エンティティ(controlling entity)によって指令され、これはBIAのシリアルライン上でコマンドを発行し、結果を受け取る。

BIAのハードウェアには4つの基本バージョン、すなわち、標準、ワイヤレス、一体型電話／ケーブルテレビ(すなわち「CATV」)／ファックス、およびATMがある。BIAハードウェアの各変形体は、市場の特定のニーズに対処し、構成に相違があるため、各変形体のセキュリティのレベルは異なる。

B I Aソフトウェアには7つの基本バージョン、すなわち、パーソナルコンピュータ（すなわち「P C」）、小売、A T M、登録、インターナル（internal）、発行者、および集積型リモート（integrated remote）がある。各ソフトウェアをロードすると、異なった、特定の用途のためのコマンドのセットが提供される。例えば、登録ソフトウェアをロードすると、小売トランザクションのメッセージを形成するリクエストは受け付けられない。同様に、小売ソフトウェアのコマンドセットは個人の登録メッセージを送ることはできない。別のセキュリティ層を提供するために、D P Cは各B I Aにどのソフトウェアパッケージがロードされているかを知っており、B I Aによる、通常送ることのできないメッセージを送ろうとする試みはいかなるものであれ拒絶され、重大なセキュリティ違反として扱われる。

B I Aの外付けインターフェースは厳しく限定されているため、B I Aの構成により、そのコンテンツを不正改変することは極度に困難になる。さらに各B I Aは、D P Cしか知らない固有の暗号化コードを持っており、各B I Aはそれに指定された機能に限定された動作しか行えないようになっている。各バイオメトリック入力手段は、D P Cに予め登録されたハードウェア識別コードを有しており、このためバイオメトリック入力手段は、そのバイオメトリック入力デバイスからの後続する各転送において、D P Cにとって一意に識別できるものとなる。

ターミナルのレンジは、パーソナルコンピュータ上で動作するソフトウェアアプリケーションから、小売P O Sのような特定の用途に開発された専用ハードウェア／ソフトウェアシステムにまで至る。特定のモデルにかかわらず、暗号化されていないバイオメトリック情報を漏らすB I Aはない。表示手段のないB I Aモデル（例えばL C D、L E Dあるいはクォーツスクリーン）は、表示用ターミナルに、選択された情報（例えば個人プライベートコード）を明らかにしなければならず、その結果、それらの特定のターミナルーB I Aの組み合わせは、安全性が劣ると考えられている。

当面のタスクにより、B I Aモデルは、部分的にあるいは完全にターミナルと一体化される。部分的に一体化されているデバイスは、ターミナルと物理的に離

れており、それらはワイヤレスおよび標準小売POSのBIAを含む。完全に一体化されたデバイスは、例えばATMや電話のようなターミナル自体に物理的に包含されている。BIAは、いかなる外部のソースにであれ、秘密の暗号化コードを明らかにすることはない。

BIAモデル

具体的なBIAハードウェアモデルは、異なる構成を有する。以下にそれらを簡単に紹介する。

BIA

標準モデルは、演算モジュール（すなわち、マルチチップモジュール）、バイオメトリックスキャナ（すなわち、単一の指紋スキャナ）、表示手段（すなわち、LCDスクリーン）、通信ポート（すなわち、シリアルポート）、不正改変不可能

なケースの中に包まれたデータエントリ手段（すなわち、マニュアルデータエントリキーボードまたはPICパッド）、および電子検出手段（すなわち、RFシールド）を有する。

BIA/ワイヤレス

標準モデルであって、シリアルラインが、外部アンテナを用いる広スペクトル（spread-spectrum）ワイヤレス通信モジュールに置き換わった標準モデル。レストランPOS（point of sale）において用いられる。

BIA/ATM

マルチチップモジュールと共に、ヘビーデューティスキャナおよびシリアルポートを有する。LDCがターミナルの一部であってBIA手段の一部ではないという事実は、セキュリティを低下させる。なぜなら、LCDは、秘密コードをターミナルへ知らせなければいけないから。ATMにおいて用いられる。

BIA/Catv

ライトデューティスキャナを有する。それ以外はATMと同様である。電話、CATVリモート、およびファクスマシンにおいて用いられる。LCDおよびPICパッドがターミナルの一部であってBIAの一部ではないために、さらに市

場の低コスト性 (low-cost nature) のために、最もセキュリティが弱い。

B I A コマンドセットメッセージ

それぞれの B I A ソフトウェアコマンドセットは、動作の異なるセットを提供する。以下にそれらを簡単に紹介する。

B I A / A T M

アカウントアクセス (Account Access)

B I A / C a t v

遠隔取引承認 (Remote Transaction Authorization)

B I A / ファクス

安全ファクス提出 (Secure Fax Submit)

安全ファクスデータ (Secure Fax Data)

安全ファクス追跡 (Secure Fax Tracking)

安全ファクス取り出し (Secure Fax Retrieve)

安全ファクス拒否 (Secure Fax Reject)

安全ファクスアーカイブ (Secure Fax Archive)

安全ファクス契約受諾 (Secure Fax Contact Accept)

安全なファクス契約拒否 (Secure Fax Contact Reject)

電子ドキュメントアーカイブ取り出し (Electronic Document Archive Retrieve)

B I A / 内部

個人の識別 (Individual Identification)

B I A / 発行者

発行者バッチ (Issure Batch)

B I A / P C

電子ドキュメント提出 (Electronic Document Submit)

電子ドキュメントデータ (Electronic Document Data)

電子ドキュメント追跡 (Electronic Document Tracking)

電子ドキュメント取り出し (Electronic Document Retrieve)

電子ドキュメント拒否 (Electronic Document Reject)

電子ドキュメントアーカイブ (Electronic Document Archive)

電子ドキュメントアーカイブ取り出し (Electronic Document Archive Retrieve)

電子署名サブミッション (Electronic Signature Submission)

電子署名チェック (Electronic Signature Check)

遠隔取引承認 (Remote Transaction Authorization)

ネットワーククレデンシャル (Network Credential)

保護された接続 (Secured Connection)

B I A / 登録

個人の識別 (Individual Identification)

バイオメトリック登録 (Biometric Registration)

B I A / 小売

取引承認 (Transaction Authorization)

I A ハードウェア：標準モデル

標準 B I A ハードウェアは、固い不正改変不可能なケースの中に包まれた単一のプリントスキャナ、LCD スクリーン、シリアルポート、および P I C パッドと組み合わされたマルチチップモジュールである。固い不正改変不可能なケースは、コンテンツのための R F シールドを提供するとともに、侵入する企てを明白にさせる。

次のコンポーネントは、B I A マルチチップモジュール（当該分野において公知な、いくつかのプロセッサを一つの物理シェルに閉じ込めるためのプロセス）と呼ばれるマルチチップモジュールに合併されている。マルチチップモジュールは、デバイス間の通信経路を簡単な傍受から防護するように構築されている。

- ・ シリアルプロセッサ
- ・ P I C パッドプロセッサ
- ・ L C D スクリーンプロセッサ
- ・ C C D スキャナ A / D プロセッサ

- ・フラッシュおよびマスクROMの両方を含む高速DSPプロセッサ
- ・汎用マイクロプロセッサ

- ・標準RAM
- ・EEPROM

次のソフトウェアパッケージおよびデータは、マスクROMに記憶されている。マスクROMは、読み出し専用メモリの他のタイプよりも安価であるが、しかしリバーシエンジニアされやすく、そして電子的に消去することができない。そのようなものとして、ここでは重要でない一般に利用可能なコードを並べるにとどめる。（マスクROMは当該分野において公知である）。

- ・MAC計算ライブラリ
- ・DUKPT鍵管理ライブラリ
- ・DES（CBSともに）暗号化ライブラリ
- ・Base-64（8ビットから印刷可能なASCIIへの）コンバータライブラリ
- ・公開鍵暗号化ライブラリ
- ・埋込みオペレーティングシステム
- ・シリアルラインデバイスドライバ
- ・LCDデバイスドライバ
- ・PICパッドデバイスドライバ
- ・スキャナデバイスドライバ
- ・ユニークハードウェア識別（identification）コード
- ・マルチ言語プロファイル

次の標準データおよびソフトウェアパッケージはフラッシュROMにおいて記憶される。フラッシュROMは、より高価であるが、リバーシエンジニアすることがさらにより困難であり、そして最も重要なことだが、電子的に消去可能である。より重要な情報の全てはここに記憶される。フラッシュROMは、BIAを複製することの困難さを増加させる試みで用いられる。（フラッシュROMは、当該分野において公知である）。

- ・ユニークDUKPT未来鍵（future key）テーブル

- ・ユニーク112-ビットMAC鍵

- ・DSPバイオメトリック品質 (biometric quality) 決定アルゴリズム
- ・DSPバイオメトリックコード化 (encoding) アルゴリズム
- ・乱数発生アルゴリズム
- ・コマンドファンクションテーブル

BIAからメッセージが送られる毎にインクリメントされるメッセージシーケンス番号は、EEPROMにおいて記憶される。EEPROMは、何回も消去されてもよいが、しかし非揮発性である—そのコンテンツは、電源の遮断を越えて有効のままである。(EEPROMは、当該分野において公知である)。

次のデータはRAMにおいて記憶されている。RAMは、性質上一時的であり、電源が失われた場合は、いつでも失われる。

- ・コード化されたバイオメトリックレジスタ (Encoded Biometric Register)
- ・PICレジスタ (PIC Register)
- ・アカウントインデックスコードレジスタ (Account Index Code Register)
- ・タイトルインデックスコードレジスタ (Title Index Code Register)
- ・アマウントレジスタ (Amount Register)
- ・ドキュメント名レジスタ (Document Name Register)
- ・PIC-ブロック鍵 (PIC-Block Key)
- ・メッセージ鍵 (Message Key)
- ・レスポンス鍵 (Response Key)
- ・共有セッション鍵 (Shared Session Key)
- ・秘密セッション鍵 (Private Session Key)
- ・8汎用レジスタ (8 General Registers)
- ・スタックおよびヒープ空間 (stack and heap space)

それぞれのマルチチップモジュールは、フラッシュROMの初期化に続いて不可逆にセットされる「一度の書き込み (write-once)」メモリロケーションを含

む。フラッシュROMへソフトウェアをダウンロードする試みが行われた場合にはいつでも、このメモリロケーションはチェックされる。もし、それがすでにセ

ットされていたならば、その後、BIAはロードすることを拒否する。この方法で、重要なソフトウェアおよびデータ鍵は、製造時に一度だけ、デバイスにダウンロードされうる。

次の関連するハードウェアコンポーネントは、標準BIAハードウェアモジュールを備える。

- ・ BIA マルチチップモジュール (BIA Multichip module)
- ・ CCD シングループプリントスキャナ (CCD single-print scanner)
- ・ 容量検出板 (capacitance detector plate) (当該分野において公知)
- ・ 照明されたPICキーパッド (lighted PIC keypad)
- ・ 2-ライン40-カラムLCDスクリーン (2-line 40-column LCD screen)
- ・ RF シールド (RF shielding)
- ・ 不正改変不可能なケース (tamper-resistant case)
- ・ シリアルコネクション (57.6kbまで) (serial connection)
- ・ ブリーチ検出ハードウェア (breach detection hardware) (当該分野において公知)
- ・ マルチチップモジュールに取り付けられた、選択可能なテルミットチャージ (thermite charge) (当該分野において公知)

これらの値を計算するために用いられる、全ての一時記憶手段および内部ハードウェアおよびソフトウェアは、保護される。このことは、それらが、それらの現在の値、または機能に関するそれらの意味を決定するいかなる試みにも耐える。この特徴は、この発明のセキュリティにとって本質的である。BIAの「傍受」や、そして特に、不正手段のためのバイオメトリックPICブロックの収集が可能な限り困難にされることが、まさに重要だからである。

マルチチップモジュールとコンポーネントとは、実際には、露出した配線が存在することなく、物理的に接続されている。

B I Aの電子コンポーネンツを防護しているエンクロージャーは、製造中に溶接されて蓋をされる。それは、ケースへの重大なダメージなしでは、いかなる状況下でも開けられ得ない。エンクロージャーのいかなる開封（またはダメージ）を

検出した際には、B I Aは、フラッシュROMにある、いかなる全ての鍵について緊急電子的ゼロ（emergency electronic zero）を実行し、その次に、ソフトウェアライブラリの全てについて実行する。特定のブリーチ（breach）検出メソッドは、極秘かつ独占（Proprietary）を維持される。

コンテンツを防護することに加えて、ケースは、RF信号検出器から、内部動作をシールドする。

B I Aの超安全な（supersecure）バージョンが存在し、それによってブリーチ（breach）検出メソッドは、検出メソッドそれ自体だけでなくマルチチップモジュールをも物理的に破壊する機構に接続されている。

B I Aハードウェア：ワイヤレスモデル

B I Aハードウェアのワイヤレスバージョンは、それが、外部シリアルポートの代わりに、外部アンテナを用いた広スペクトルワイヤレス通信モジュールをエクスポートすることを除いて、構造上標準モデルと同じである。

このバージョンは、レストランにおいて用いられるように設計されている。レストランでは、顧客の都合に合わせて、取引が承認される。

次の記述において、標準セットに追加されるアイテムは、＋文字によって表記される。一方、標準セットから除去されるアイテムは、－文字によって表記される。

マルチチップモジュール：

- ・ドキュメント名レジスタ（Document Name Register）
- ・共有セッション鍵（Shared Session Key）
- ・秘密セッション鍵（Private Session Key）
- ・メッセージ鍵（Message Key）

コンポーネンツ：

- ・シリアルポート (Serial port)
- ・外部アンテナ (External antenna)

- ・広スペクトルワイヤレスシリアルモジュール (当該分野において公知)

B I Aハードウェア：A T M (自動テラーマシン) モデル

B I AハードウェアのA T Mバージョンは、ヘビーデューティシンググループプリントスキャナ (heavy-duty single-print scanner) とシリアルポートとに結合されたマルチチップモジュールである。コンポーネントは、不正改変不可能なケースの中に包まれる。不正改変不可能なケースは、コンテンツのためのR Fシーールドを提供するとともに、侵入する企てを明白にさせる。

このバージョンは、A T Mの位置において改裝されるように設計される。そのようなものとして、スキャナパッドは、ヘビーデューティセンサパッドであり、全体の構造は、A T Mそれ自体において存在するスクリーンおよびキーパッドを利用する。

次の記述において、標準セットに追加されるアイテムは、＋文字によって表記される。一方、標準セットから除去されるアイテムは、－文字によって表記される。

マルチチップモジュール：

- ・アマウントレジスタ (Amount Register)
- ・ドキュメント名レジスタ (Document Name Register)
- ・共有セッション鍵 (Shared Session Key)
- ・秘密セッション鍵 (Private Session Key)
- ・メッセージ鍵コンポーネント： (Message Key Components:)
- ・照明されたP I Cキーパッド (lighted P I C keypad)
- ・2－ライン40－カラムL C Dスクリーン (2-line 40-column L C D screen)

A T MはL C DスクリーンまたはP I Cキーパッドを有さないので、実は、マスクROMにおいてそれらのデバイスドライバが必要ないことに注意されたい。

B I Aハードウェア：電話／C A T Vモデル

B I Aハードウェアの電話／C A T Vバージョンは、シングループリントスキャナ

(single-print scanner) とシリアルポートとに結合されたマルチチップモジュールである。モジュールは、物理的にスキャナに取り付けられており、全体は、干渉を行うのをより困難にするために、プラスチックの中に包まれている。かなりの量のR Fシールドがコンポーネントのために提供される。

このバージョンは、電話機、テレビジョンリモートコントロールおよびファクスマシンと一体化されるように設計される。結果として、それは、存在するキーパッド、L C Dまたはテレビジョンスクリーンを利用して、値をエンターまたは表示する。また、それはホストターミナルの通信機能を使う。例えば、ファクスマシンはビルトインファクスモデムを用い、テレビジョンリモートは、C A T Vケーブルネットワークを用いる。

このハードウェアモデルは、(他のモデルと比較して) 比較的安全性が低い。それらのデバイスが、可能な限りコストがかからず、軽重量であり、存在する低コストデバイスと容易に一体化できるように意図されるからである。

次の記述において、標準セットに追加されるアイテムは、+文字によって表記される。一方、標準セットから除去されるアイテムは、-文字によって表記される。

マルチチップモジュール：

- ・ドキュメント名レジスタ (Document Name Register)
- ・共有セッション鍵 (Shared Session Key)
- ・秘密セッション鍵 (Private Session Key)
- ・メッセージ鍵 (Message Key)

コンポーネント：

- ・照明されたP I Cキーパッド (lighted P I C keypad)
- ・2-ライン40-カラムL C Dスクリーン (2-line 40-column L C D screen)

B I Aソフトウェア

B I A ソフトウェアコマンドインターフェイス

B I A への外部インターフェイスは、標準モデムによく似ている。外部シリアルラインを用いて、コマンドが制御ターミナルから B I A に送られる。コマンドが完了した場合、レスポンスコードが B I A からターミナルへ送られる。

それぞれの B I A ソフトウェアロード (software load) は、動作の異なるセットをサポートする。例えば、小売ロード (retail load) は、取引承認だけをサポートし、一方、登録ロード (registration load) は、個人の識別 (identification) およびバイオメトリック登録をサポートする。

全ての B I A データフィールドは、プリント可能な A S C I I の形態であり、fs制御文字で分離されたフィールド、および復帰改行 (newlines) によって分離されたレコードとを有する。暗号化されたフィールドは、base-64変換ライブラリを用いて64ビット A S C I I に変換されたバイナリである（これらは当該分野において公知である）。

いくつかのコマンドは、いくつかの構成において利用できない。例えば、A T M B I A は、「Get P I C」できない。なぜなら、P I C パッドが取り付けられていないから。そのかわり、A T M B I A は、「Set P I C」コマンドをサポートする。

レスポンスコード：

時間切れ：

コマンドに割り当てられた時間が満了した。その効果に対するメッセージが、L C D スクリーンが利用可能ならば、それ上に表示される。所定のコマンドに対して時間が満了した場合、B I A は、キャンセルボタンが押されたかのように動作する。

キャンセルされた：

キャンセルボタンが押され、そして全動作がキャンセルされた。これは、集められた全ての情報を取り除くという副効果を有する。その効果に対するメッセージが、L C D スクリーンが利用可能ならば、それ上に表示される。

Ok：

コマンドが成功した。

その他：

それぞれのコマンドが、それに対してのみ有効な、特定の他のレスポンスコードを有してもよい。これらのレスポンスコードは一般に、コードに付随するテキストを有してもよい。テキストは、LCDスクリーンが利用可能ならば、それ上に表示される。

メッセージ：

これは、コマンドが進行中であることを示し、しかしBIAがターミナルに中間結果のメッセージを送りたいことを示す。この結果は、また、LCDスクリーンが利用可能ならば、それ上に表示される。この機能は、ステータスメッセージだけでなくプロンプトのためにも用いられる。

コマンド

以下のコマンドの引数 (argument) リストにおいて、〈〉の文字で個々の引数を囲み、[]の文字でオプションな引数を囲み、|の文字は、ある引数が示された選択肢のうちの1つからなり得ることを示す。

Set language 〈言語名〉

このコマンドは、ユーザ入力を促す (prompt) ための、BIA内で符号化される複数の異なる言語のうち1つを選択する。

Get Biometric 〈時間〉 [1次 | 2次]

このコマンドは、BIAに、そのスキャナを作動させて、個人からバイオメトリック入力を得て、符号化バイオメトリックレジスタに格納することを要求する。

まず、「点灯したパネル上に指をおいて下さい」のメッセージがLCDパネル上に表示され、ターミナルに返される。スキャナパッドが照明されて、個人がそのバイオメトリックをエンターするように促す。

〈時間〉値がゼロであることは、バイオメトリックスキャン入力に時間制限がないことを意味する。

スキャニングモードにおいて、指紋スキャンがとられ、紋品質アルゴリズム(p

rint quality algorithm)によって予備分析がなされる。スキャンが十分よくない場合は、B I Aは〈時間〉秒が経過するまで新しいスキャンをとり続ける。時間が経過して紋のスナップショットがとられて分析されると、メッセージがLCDスクリーンに掲示されて、紋品質ソフトウェアによって検知された問題に基づきターミナルに送られる。適切な品質の紋が得られない場合は、B I Aは時間が過ぎたことを示すエラーコードを返し、その旨のメッセージをLCD上に表示する。

紋品質アルゴリズムが紋スキャンの品質を是認(affirm)すると、紋の詳細(minutiae)が紋符号化アルゴリズムによって抽出される。識別に十分な量を保持するように注意しながら、詳細の部分集合のみをランダムに選択する。次に詳細をランダムに並べ、符号化バイOMETリックレジスタに入れる。すると、B I Aは成功結果コードでもって応答する。

もし「1次」2次」が指定されていれば(バイOMETリック登録コマンドセットにおいてのみ利用可能)詳細セットの小さな部分集合だけでなくその全体が選択される。同様に、1次/2次バイOMETリック選択は、符号化されたバイOMETリックを適切なレジスタに入れることになる。

動作が成功するか否かに関わらず、スキャンが終わるとともに、スキャンが進行中であることを示すライトが消灯される。

同じバイOMETリック入力異なる符号結果(encoding)を生み出すことにより、手に入れた(capture) B I Aの暗号化コードを発見しようとする者の作業を複雑にすることが非常に重要である。これは、ランダムな部分集合を選択し、符号化バイOMETリックをランダムに並べることにより、達成される。

Get PIC 〈時間〉

このコマンドは、B I Aがキーパッドからの読み取りを行うことによってPICレジスタを埋めることを要求する。

まず、「あなたのPICを入力してから〈エンター〉を押して下さい」のメッセージがLCDディスプレイ上に表示されてターミナルに送られ、適切なキーパッドライトが点灯され、次にキーパッドスキャンが開始される。

〈時間〉秒数が切れたときか、個人が〈エンター〉キーを押したときに、スキニングが終了する。

P I Cの個々の数字はL C D上に表示されず、個々がタイプする各数字に対して星印「*」が現れることにより個人にフィードバックを行う。「訂正」キーが押されたとき、最後にエンターされた数字が消去され、個人が入力ミス直すことを可能にする。

P I C入力が終了すると、キーパッドライトが消灯する。

成功すれば、コマンドはO Kを返す。

Get Account Index Code 〈時間〉

まず、「ではあなたのアカウントインデックスコードを入力してから〈エンター〉を押して下さい」のメッセージがL C D上に表示されてターミナルに送られる。これにより、個人は自分のアカウントインデックスコードをエンターするように促される。各キーが押されたとき、その値がL C Dパネル上に現れる。訂正ボタンをおすことによって値のうち1つを消去することかできる。「エンター」ボタンが押されると、アカウントインデックスコードレジスタがセットされる。

入力中、適切なキーパッドのキーが点灯され、入力が完結したとき、キーパッドのライトが消灯される。

成功すれば、コマンドはO Kを返す。

Get Title Index Code 〈時間〉

まず、「あなたのタイトルインデックスコードを入力してから〈エンター〉を押して下さい」のメッセージがL C D上に表示されてターミナルに送られる。これにより、個人は自分のタイトルインデックスコードをエンターするように促される。各キーが押されたとき、その値がL C Dパネル上に現れる。訂正ボタンをおすことによって値のうち1つを消去することができる。「エンター」ボタンが

押されると、タイトルインデックスコードレジスタがセットされる。

入力中、適切なキーパッドのキーが点灯され、入力が完結したとき、キーパッドのライトが消灯される。

成功すれば、コマンドはO Kを返す。

Validate Amount 〈金額〉 〈時間〉

Validate Amount コマンドは、「金額 〈金額〉 OK？」のメッセージをターミナルに送り、これをLCDスクリーン上に表示する。もし個人が「はい」（またはエンター）ボタンを押すことにより金額を確認すれば、金額レジスタが〈金額〉にセットされる。〈金額〉値は、制御文字やスペースなどの無い、有効な数字でなければならない。プロンプトを出している間、はい、いいえ、およびキャンセルボタンが点灯される。プロンプトが完了すると、全てのライトが消灯される。

もし個人が「いいえ」をエンターすると、トランザクションはキャンセルされる。

Enter Amount 〈時間〉

Enter Amount コマンドは、「金額を入力して下さい」のメッセージをターミナルに送り、これをLCDスクリーン上にも表示する。個人は次にドル金額を自分でエンターしなければならない。エンターされた各文字は、LCDスクリーン上に表示される。全ての適切なボタンが点灯される。エンターボタンが押されると、金額レジスタがキーボード上でエンターされた値にセットされる。入力が完了すると、全てのライトが消灯される。

Validate 文書 〈名称〉 〈時間〉

Validate Document コマンドは、「文書 〈名称〉 OK？」のメッセージをターミナルに送り、これをLCDスクリーン上にも表示する。もし個人が「はい」（またはエンター）ボタンを押すことにより文書を確認すれば、文書名レジスタが〈名称〉にセットされる。〈名称〉値は、制御文字や前後のスペースなどの無い、印刷可能なASCII文字でなければならない。プロンプトを出している間、はい、

いいえ、およびキャンセルボタンが点灯される。プロンプトが完了すると、全てのライトが消灯される。

もし個人が「いいえ」をエンターすると、トランザクションはキャンセルされる。

Assign Register 〈レジスタ〉 〈テキスト〉

assign register コマンドは、指定された一般〈レジスタ〉を値〈テキスト〉

を有するようにセットする。これは、マーチャントコード、製品情報などの情報をセットするために用いられる。

Get Message Key

Get Message Keyコマンドは、B I Aに、制御装置がメッセージに追加したい任意のメッセージ本体を暗号化するために制御ハードウェアが使用する、56ビットランダム鍵を生成させる。生成された鍵は、16進数フォーマット（当該分野では公知）でB I Aに返される。メッセージ鍵が次にバイオメトリックP I Cブロックに追加される。

Form Message <タイプ識別 | トランザクション | アカウントアクセス...>

Form Messageコマンドは、B I Aに、集めた全ての情報を含むメッセージを出力するように命令する。また、その特定のメッセージ<タイプ>に適切な全てのレジスタがセットされたことを確実にするためチェックする。もし全てのレジスタがセットされていなければ、B I Aはエラーを返す。特定のコマンドセットソフトウェアが、そのB I Aモデルによってどのメッセージが形成され得るかを決定し、その他は全て拒否される。

各メッセージは、B I Aの固有のハードウェア識別コードからなる送信コードおよび、インクリメントするシーケンス番号を含んでいる。送信コードは、送っているB I AをD P Cが識別し、再入力攻撃(resubmission attack)を検知することを可能にする。

B I Aは、D U K P T鍵管理システムを用いて、将来鍵テーブルからバイオメトリックP I Cブロック暗号化56ビットD E S鍵を選択する。この鍵は次に、暗号化ブロックチェイニング(C B C)(cipher block chaining)を用いてバイオメトリックP I Cブロックを暗号化するために使用される。また、レスポンスD E S鍵もランダムに生成され、レスポンスの中で暗号化される必要のある部分を暗号化するためにD P Cによって使用される。

注：レスポンス鍵をバイオメトリックP I Cブロック鍵は、非常に重要である。なぜなら、各暗号化鍵はその責任範囲でのみ使用されなければならないからである。このようにすれば、もし何者かが秘密コードを符号化している鍵を破る

うとしても、バイオメトリックP I Cの露呈には至らない。

B I A - P I Cブロックの構成フィールド：

- ・ 3 0 0 バイト承認バイオメトリック
- ・ 4 - 1 2 桁 P I C
- ・ 5 6 ビットレスポンス鍵
- ・ [オプションな 5 6 ビットメッセージ鍵]

メッセージ鍵は、制御ターミナルがこのメッセージに対するメッセージ鍵を要求した場合にのみ存在することに注意せよ。メッセージ鍵を用いてトランザクション承認リクエストに添付されたメッセージ本体の暗号化は、制御ターミナルに委ねられる。

全ての暗号化が完了すると、B I A は、メッセージ承認コード (M A C) によって終了かつ保護される、適切なリクエストメッセージ (例えばトランザクション承認リクエストメッセージなど) の本体を出力する。

M A C フィールドは、B I A のシークレット 1 1 2 ビット D E S M A C 鍵を用いて計算され、1 番目から最後まで全てのメッセージフィールドをカバーする。M A C は、制御ターミナルが平文フィールドを検査 (inspect) することを可能にしながら、メッセージ内に、効果的にメッセージを密封することを変更するものは何もなかったことを、D P C に対して保証する。

Form Message コマンドが実行されると、B I A は、「D P C 中央と通話しています」のメッセージをターミナルに送り、L C D スクリーンにもこれを表示し、作業がリクエストに対して進行中であることを示す。

コマンドが完了すると、コマンドは、形成されたメッセージ全体を返すとともに O K を返す。

Show Response 〈暗号化レスポンス〉 〈時間〉

Show Response コマンドは、B I A に、その現在のレスポンス鍵を用いてシステムから秘密コードを復号化するように命令する。

復号化後、チャイムが鳴り、秘密コードが L C D スクリーンに 〈時間〉 秒間表示される。このコマンドは、復号化された秘密コードを制御ターミナルに送信す

ることは、いかなる時点においても無い。

Validate Private 〈復号化された有効性証明〉 〈時間〉

このコマンドは、安全なネットワーク通信セッション中において、個人に外部ソースからのメッセージを有効性証明するように依頼するために、ターミナルによって用いられる。メッセージは、暗号化され、かつチャレンジおよびレスポンスの2部分に分けてやって来る。

Validate Privateコマンドを受け取った際、B I Aは、チャレンジメッセージのテキストを、「OK 〈チャレンジ〉？」のようにLCD上に表示するが、ターミナルにはこれを送らない。個人がチャレンジを有効性証明したとき、レスポンスがB I Aによって秘密セッション鍵を用いて暗号化され、OKレスポンスコードとともにターミナルに返される。個人がチャレンジの有効性証明をしなかったとき、B I Aは、LCDスクリーンにも表示される「あなたのリクエストによりトランザクションをキャンセルしました」というテキストとともに、「失敗」レスポンスコードを返す。

ターミナルは、チャレンジまたはレスポンスの平文を見ることを許可されることは決してないことに注意せよ。

Reset

Resetコマンドは、B I Aに、全ての一時的レジスタLCDスクリーン、全ての一時的鍵レジスタをクリアし、点灯している可能性のある全てのキーパッドラ

イトを消灯するように命令する。

Set P I C 〈値〉

このコマンドは、B I AのP I Cレジスタを〈値〉に割り当てる。安全にされていない(non-secured)装置がP I Cを提供することを許すことは、セキュリティ問題になる可能性があることに注意せよ。なぜなら、安全にされていない装置は、盗聴または交換にあう危険性がずっと大きいからである。

Set Account index code 〈値〉

このコマンドは、B I Aのアカウントインデックスコードレジスタを〈値〉に割り当てる。安全にされていない装置がアカウントインデックスコードを提供す

ることを許すことは、セキュリティ問題になる可能性があることに注意せよ。なぜなら、安全にされていない装置は、盗聴または交換にあう危険性がずっと大きいからである。

Set Title Index Code 〈値〉

このコマンドは、B I Aのタイトルインデックスコードレジスタを〈値〉に割り当てる。安全にされていない装置がタイトルインデックスコードを提供することを許すことは、セキュリティ問題になる可能性があることに注意せよ。なぜなら、安全にされていない装置は、盗聴または交換にあう危険性がずっと大きいからである。

Set金額 〈値〉

このコマンドは、B I Aの金額レジスタを〈値〉に割り当てる。

Decrypt Response 〈暗号化されたレスポンスメッセージ〉

Decrypt Responseコマンドは、B I Aに、その現在のレスポンス鍵を用いてレスポンスメッセージの暗号化された部分を復号化するように命令する。復号化がなされると、レスポンスは制御装置に返され、おそらくはA T MターミナルのL

E Dスクリーン上に表示される。

この復号能力を提供することはセキュリティ問題である。なぜなら、ターミナルは、平文がB I Aを離れると、それを用いてそれが行うであろうことを行う能力を有するからである。

B I Aソフトウェア：サポートライブラリ

B I Aソフトウェアは、いくつかの異なるソフトウェアライブラリによってサポートされる。そのいくつかは標準的、一般に利用可能なライブラリであるが、またいくつかは、B I Aに関して特別な要求事項を有するものである。

乱数発生器

B I Aは、メッセージ本体およびメッセージレスポンス暗号化に使用するために、常にランダムなD E S鍵を選択しているため、選択された鍵が予測不可能な鍵であることが重要である。もし乱数発生器が1日の時刻あるいはその他の外部的に予測可能なメカニズムによっていると、暗号化鍵はそのアルゴリズムを知っ

ている敵による類推がずっと容易になってしまう。B I Aで用いる暗号化技術のセキュリティを確実にするために、乱数発生器アルゴリズムと暗号化アルゴリズムの両方とも公知であると仮定する。

D E S 鍵を生成するための標準的な乱数発生アルゴリズムは、A N S I X 9 . 1 7、appendix C（当該技術において公知）中に定義されている。

D S P バイオメトリック符号化アルゴリズム

バイオメトリック符号化アルゴリズムは、人間の指先上の、うね(ridge)の終わりがたおよび分岐によって形成される詳細を探すための、専用の(proprietary)アルゴリズムである。詳細の完全なリストがD P C 内にリファレンスとして格納されている一方、識別候補と登録された個人との間の比較を行う際には、部分的なリストのみしかアルゴリズムは要求しない。

バイオメトリック登録および識別の両方の際において、符号化アルゴリズムは、バイオメトリック入力ステップが終わるまでに十分な詳細が見つけれらる(found)

d) ことを確実にする。

オペレーティングシステムおよびデバイスドライバ

B I A はリアルタイム計算環境であり、そのため、それを実行するためのリアルタイム埋め込みオペレーティングシステムが必要である。オペレーティングシステムは、装置から割り込み(interrupt)をとり、タスクをスケジューリングする役目を果たす。

各デバイスドライバは、オペレーティングシステムと特定のハードウェアとの間のインターフェースの役割を果たす。例えばP I C パッドデバイスドライバやC C D スキャナデバイスドライバである。ハードウェアは、「P I C パッドキーが押された」や「C C D スキャナのスキャンが完了した」などのイベントの源である。デバイスドライバは、そのような割り込みを扱い、イベントを解釈し、イベントに対するアクションを行う。

D E S 暗号化ライブラリ

D E S のインプリメンテーションは公知のものがいくらかでもある。D E S のイ

ンプリメンテーションは、56ビットシークレット鍵を用いて、平文から暗号文(ciphertext)へのシークレット鍵型暗号化および、暗号文から平文への復号化を、提供する。

公開鍵暗号化ライブラリ

公開鍵暗号化サポートライブラリは、RSA公開鍵特許(当該分野で公知)の所有者であるPublic Key Partnersから入手可能である。公開鍵暗号システム(Public Key cryptosystem)は、コストがかかるシークレット鍵の交換を必要とすることなしに通信することを可能にする、非対称暗号化システムである。公開鍵暗号化システムを使用するためには、公開鍵を用いてDES鍵を暗号化し、次にDES鍵を用いてメッセージを暗号化する。BIAは、公開鍵暗号システムを用いて、シークレット鍵の安全な交換を可能にする。

残念なことに、公開鍵システムはシークレット鍵システムよりもテストが非常に遅れており、そのためこの種のアプローチ全体に対する信頼レベルが低い。従って、本発明は、公開鍵暗号作成法を、通信セキュリティおよび短期信用情報交換(credential exchange)に用い、秘密(secrets)の長期保存には用いない。ネットワーククリデンシャルを作成するために、エンドユーザー個人および銀行の両方が、DPCによって識別される。ネットワーククリデンシャルは、エンドユーザー個人の識別ならびに、接続の文脈(すなわちTCP/IPソースおよび行先ポート(destination port))を包含する。

DUKPT鍵管理ライブラリ

最初の鍵と、メッセージシーケンス番号が与えられれば、ドライブドユニーク鍵／トランザクション(DUKPT)管理を用いて、将来のDES鍵を作成する。将来の鍵は、将来鍵テーブルに格納されている。ある鍵は、いったん使用されるとテーブルからクリアされる。最初の鍵は、最初の将来鍵テーブルを作成するためのみに用いられる。従って、最初の鍵はBIAに格納されない。

DUKPTの使用は、最初の鍵を痕跡を残すことなく、各トランザクションに対して異なるDES鍵を提供する鍵管理メカニズムを作成することを意図している。この意味するところは、もし将来鍵テーブルがうまく手に入れられて解体(d

issect)されたとしても、以前に送られたメッセージが曝露されることはないということであり、送信される情報の寿命が何十年にもなる場合には、これは非常に重要なゴールである。D U K P Tは、A N S I X 9. 2 4 (当該分野において公知) に完全に規定されている。

D U K P Tはもともと、デビットカード(debit card)トランザクション用の、P I C暗号化メカニズムをサポートするために開発された。この環境においては、全てのトランザクションを保護することが重要であった。犯罪者が、6ヶ月間暗号化トランザクションを記録して、P I Cパッドを手に入れそこから暗号化コードを抽出するのに成功したと仮定する。すると犯罪者は、その6ヶ月間の間に送信された各メッセージに対して、1つの新しい偽造デビットカードを製造することができる。しかしD U K P T下においては、犯罪者の窃盗および解体によって以前のメッセージが復号化されることはない(ただし犯罪者が解体後にP I Cパ

ッドを交換したとすれば新しいメッセージは依然として復号化可能である)

バイオメトリックP I C状況においては、犯罪者にとってより困難性が増す。なぜなら、メッセージが復号化されたとしても、デジタルバイオメトリックP I Cを肉体的な指紋に変換することは、アカウントナンバーP I Cをプラスチックカードに変換することよりもずっと困難であるためであり、これは、トークンレスシステムの大きな利点の1つである。

しかしながら、もし犯罪者が復号化することが可能であるならば、暗号化もできるわけであり、バイオメトリックP I Cをシステムに電子的に入力して詐欺的なトランザクションを承認させることが可能かもしれない。これは非常に困難ではあるが、それでも犯罪者に利用可能なオプションはなるべく制限する方がよいため、D U K P Tを使用する。

B I Aソフトウェアコマンドセット

B I Aソフトウェア：小売コマンドセット

B I A／小売ソフトウェアインターフェースは、特定の小売P O Sターミナルがシステムと相互作用することを許すインターフェースをエクスポートする。

B I A／小売インターフェースは、ターミナルが次の動作を実行することを許すように設計されている。

取引承認

それらの動作を履行するために、B I A／小売は、次のコマンドセットを供給する。

- ・ Set Language 〈言語一名〉
- ・ Get Biometric 〈時間〉
- ・ Get P I C 〈時間〉
- ・ Assign Register 〈レジスタ〉 〈値〉
- ・ Get Account index code 〈時間〉
- ・ Validate Amount 〈アマウント〉 〈時間〉
- ・ Enter Amount 〈時間〉
- ・ Form Message 〈タイプ〉
- ・ Show Response 〈暗号化されたレスポンス〉 〈時間〉
- ・ Reset

B I Aソフトウェア：C A T V（一体化されたリモート）コマンドセット

B I A／C A T Vソフトウェアインターフェースは、電話／C A T V B I Aと一体化されたターミナルがシステムと相互作用することを許すコマンドセットをエクスポートする。次の動作がサポートされる。

遠隔取引承認

その動作を履行するために、B I A／C A T Vは、次のコマンドセットを提供する。

- ・ Get Biometric 〈時間〉
- ・ Set P I C 〈テキスト〉
- ・ Assign Register 〈レジスタ〉 〈テキスト〉
- ・ Set Account index code 〈テキスト〉
- ・ Form Message 〈タイプ〉
- ・ Decrypt Response 〈暗号化されたレスポンスメッセージ〉

- ・ Reset

B I A ソフトウェア：一体化されたファクスコマンドセット

B I A / ファクスソフトウェアインターフェースは、ファクス B I A と一体化されたターミナルがシステムと相互作用することを許すコマンドセットをエクスポートする。次の動作がサポートされる。

- ・ 安全ファクス提出 (Secure Fax Submit)
- ・ 安全ファクスデータ (Secure Fax Data)
- ・ 安全ファクス追跡 (Secure Fax Tracking)
- ・ 安全ファクス取り出し (Secure Fax Retrieve)
- ・ 安全ファクス拒否 (Secure Fax Reject)
- ・ 安全ファクスアーカイブ (Secure Fax Archive)
- ・ 安全ファクス契約受諾 (Secure Fax Contact Accept)
- ・ 安全ファクス契約拒否 (Secure Fax Contact Reject)
- ・ 電子ドキュメントアーカイブ取り出し (Electronic Document Archive Retrieve)

これらの動作を履行するために、B I A / ファクスは、次のコマンドセットを提供する。

- ・ Get Biometric <時間>
- ・ Set P I C <テキスト>
- ・ Set Title Index Code <テキスト>
- ・ Assign Register <レジスタ> <値>
- ・ Get Message Key
- ・ Form Message <タイプ>
- ・ Decrypt Response <暗号化されたレスポンスメッセージ>
- ・ Reset

B I A ソフトウェア：登録コマンドセット

B I A / Reg インターフェースは、汎用コンピュータが個人を識別し登録するようにシステムと相互作用することを許すインターフェースをエクスポートする

。次の動作がサポートされる。

個人の識別

バイオメトリック登録

それらの動作をサポートするために、B I A / Regは、次のコマンドセットを提供する。

- Set Language <言語一名>
- Get Biometric <時間> [プライマリ | セカンダリ]
- Get P I C <時間>
- Assign Register <レジスタ> <テキスト>
- Get Message Key
- Form Message <タイプ>
- Show Response <暗号化されたレスポンス> <時間>
- Reset

B I A ソフトウェア：P C コマンドセット

B I A / P C ソフトウェアインターフェースは、汎用コンピュータが電子ドキュメントを送り、受信し、電子ドキュメントに署名し、ネットワークにわたって取引きを指揮し、ネットワーク上のサイトへのバイオメトリック導出 (biometric-derived) クレデンシャルを提供することを許すコマンドセットをエクスポートする。次の動作がサポートされる。

- 電子ドキュメント提出 (Electronic Document Submit)
- 電子ドキュメントデータ (Electronic Document Data)
- 電子ドキュメント追跡 (Electronic Document Tracking)
- 電子ドキュメント取り出し (Electronic Document Retrieve)
- 電子ドキュメント拒否 (Electronic Document Reject)
- 電子ドキュメントアーカイブ (Electronic Document Archive)
- 電子ドキュメントアーカイブ取り出し (Electronic Document Archive Retrieve)
- 電子署名サブミッション (Electronic Signature Submission)

- ・電子署名チェック (Electronic Signature Check)
- ・遠隔取引承認 (Remote Transaction Authorization)
- ・ネットワーククレデンシャル (Network Credential)
- ・保護された接続 (Secured Connection)

これらの動作をサポートするために、B I A / P Cは、次のコマンドセットを提供する。

- ・ Set Language <言語一名>
- ・ Get Biometric <時間>
- ・ Get P I C <時間>
- ・ Get Account index code <時間>
- ・ Validate Amount <アマウント> <時間>
- ・ Enter Amount <時間>
- ・ Validate Document <名> <時間>
- ・ Assign Register <レジスタ> <テキスト>
- ・ Get Message Key
- ・ Form Message <タイプ>
- ・ Show Response <暗号化された応答> <時間>
- ・ Validate Private <暗号化された有効性証明> <時間>
- ・ Reset

B I A ソフトウェア：発行者コマンドセット

B I A / I ssソフトウェアインターフェースは、汎用コンピュータがバッチ変更リクエストを認証し提出するようにシステムと相互作用することを許すインターフェースをエクスポートする。次の動作がサポートされる。

発行者バッチ

この動作を履行するために、B I A / I ssは、次のコマンドセットを提供する。

。

- ・ Set Language <言語一名>
- ・ Get Biometric <時間> [プライマリ | セカンダリ]

- ・ Get P I C 〈時間〉
- ・ Assign Register 〈レジスタ〉 〈値〉
- ・ Get Message Key
- ・ Form Message 〈タイプ〉
- ・ Show Response 〈暗号化されたレスポンス〉 〈時間〉
- ・ Reset

B I A ソフトウェア：内部コマンドセット

B I A / I nt は、汎用コンピュータが個人を識別するようにシステムと相互作用することを許すコマンドセットをエクスポートする。次の動作がサポートされる。

個人の識別

この動作を履行するために、B I A / I nt は、次のコマンドセットを提供する

。

- ・ Set Language 〈言語一名〉
- ・ Get Biometric 〈時間〉
- ・ Get P I C 〈時間〉
- ・ Assign Register 〈レジスタ〉 〈値〉
- ・ Get Message Key
- ・ Form Message 〈タイプ〉
- ・ Show Response 〈暗号化されたレスポンス〉 〈時間〉
- ・ Reset

B I A ソフトウェア：A T M コマンドセット

B I A / A T M ソフトウェアインターフェースは、A T M が個人を識別 (identify) することを許すコマンドセットをエクスポートする。次の動作がサポートされる。

アカウントアクセス

この動作を履行するために、B I A / A T M は次のコマンドセットを提供する

。

- ・ Get Biometric <時間>
- ・ Set P I C <テキスト>
- ・ Set Account index code <テキスト>
- ・ Assign Register <レジスタ> <値>
- ・ Form Message <タイプ>
- ・ Decrypt Response <暗号化されたレスポンスメッセージ>
- ・ Reset

ターミナル

ターミナルは、B I Aを制御し、モデム、X.25接続、またはインターネット接続（業界において公知の方法）を介してD P Cと接続する装置である。ターミナルは、異なる形状および大きさを有し、タスクを実行するために異なるバージョンのB I Aを必要とする。バイオメトリック入力装置にコマンドを発行、およびそこから答を受け取る電子装置はいずれもターミナルであり得る。

一部のターミナルは、汎用マイクロコンピュータ上でランされるアプリケーションプログラムであり、他のターミナルは、特定目的ハードウェアおよびソフトウェアのコンビネーションである。

ターミナルが、全体的にシステムの機能にとって決定的に重要である一方で、システム自体はターミナルに少しも信頼をおいていない。ターミナルがシステムに情報を提供する度に、確認のための個人への提示、または他の予め登録された情報とのクロスチェックによって、システムは常に何らかの手法によりそれを確認する。

ターミナルが、データがB I Aに適切に処理されたことを確認するためにB I Aメッセージの一部を読みとることが可能な一方で、ターミナルはバイオメトリック、P I C、暗号化鍵、またはアカウントインデックスコードを含むバイオメトリック識別情報を読みとることはできない。

特定のB I Aは、P I Cエントリ、および秘密コードディスプレイなど何らかのセキュリティ機能をターミナルにエクスポートする。その結果、そのような装置は、完全に内蔵された同一のもの(their entirely self-contained counterpa

rts)と比べて安全性が低いとみなされ、そのため結果的に低いセキュリティ評点を有することになる。

多くの異なるターミナルのタイプがあり、それぞれは特定のモデルB I Aに接続される。それぞれのターミナルを、以下に簡単に説明する。

A T M(Automated Teller Machinery)

A T Mソフトウェアのロードを伴う一体型B I A/A T Mは、A T Mキャッシュディスペンサへのバイオメトリック-P I Cのアクセスを提供する。

B R T(Biometric Registration Terminal)

マイクロコンピュータに付属するレジスタレーションソフトウェアのロードを伴う標準B I Aは、銀行に、財政アカウント評価および他の個人情報とともに新規の個人のシステムへの登録を可能にする。

C E T(Certified Email Terminal)

マイクロコンピュータに付属するP Cソフトウェアのロードを伴う標準B I Aは、個人が、認証された電子メールメッセージを送信、受信、アーカイブ化、拒

否、およびトラックすることを可能にする。

C P T(Cable-TV Point of Sale Terminal)

C A T V広帯域に付属するC A T Vソフトウェアのロードを伴うB I A/c a t vは、バイオメトリック-テレビ(または「T V」)リモコンを有する個人が、テレビショッピングでの購入を承認することを可能にする。

C S T(Customer Service Terminal)

マイクロコンピュータシステムに付属するインターナルソフトウェアのロードを伴う標準B I Aは、従業員が顧客サービスの目的でデータベースリクエストを構築することを承認する。

E S T(Electronic Signature Terminal)

マイクロコンピュータに付属するパーソナルコンピュータソフトウェアのロードを伴う標準B I Aは、個人が、書類への電子署名を構築し検証することを可能にする。

I P T(Internet Point of Sale Terminal)

マイクロコンピュータに付属するパーソナルコンピュータソフトウェアのロードを伴う標準B I Aは、インターネット接続を有する個人が、インターネットに接続したマーチャントから製品を購入することを可能にする。

I T (Issuer Terminal)

マイクロコンピュータに付属する発行者ソフトウェアのロードを伴う標準B I Aは、銀行が、資産アカウントのバッチされた変更をD P Cへ送信することを可能にする。

I T T (Internet Teller Terminal)

インターネット接続を有するマイクロコンピュータに付属するパーソナルコンピュータソフトウェアのロードを伴う標準B I Aは、個人が、所望のインターネット銀行とのトランザクションを行うことを可能にする。

P P T (Phone Point of Sale Terminal)

電話と一体化されたC A T Vソフトウェアのロードを伴うB I A / c a t vは、個人が、電話でのトランザクションを承認することを可能にする。

R P T (Retail Point of Sale Terminal)

X. 25ネットワークに付属するまたはモデムを使用するリテイルソフトウェアのロードを伴う標準B I Aは、個人が店においてトランザクション承認を使用してアイテムを購入することを許可する。

S F T (Secure Fax Terminal)

ファックスマシンと一体化されたファックスソフトウェアのロードを伴うB I A / c a t vは、個人が、安全なファックスメッセージを送信、受信、拒否、アーカイブ化、およびトラックすることを可能にする。

ターミナル：小売りPOSターミナル

RPTの目的は、個人が現金、小切手、デビットカードまたはクレジットカードのいずれをも用いる必要なく店舗で品物を購入することを可能にすることである。

RPTは、個人からマーチャントへの金銭的トランザクションを承認するためにB I A / 小売りをを用いる。RPTは、バイオメトリックPIC承認を受け入れるために用

いられることに加えて、標準のデビットカードおよびクレジットカード走査機能をも提供する。

RPTはまた、オプションのスマートカードリーダーだけでなく、標準のクレジットおよびデビット磁気ストライプカードリーダーをも含むと考えられる。

各RPTは、モデム、X.25ネットワーク接続、ISDN接続、または同様のメカニズムによりDPCに接続される。RPTはまた、トランザクションの量およびマーチャントコードが得られる電子キャッシュレジスタなどの他のデバイスにも接続され得る。

RPTの構成：

- ・ BIA／小売り
- ・ 低価格のマイクロプロセッサ
- ・ 9.6kbモデム／X.25ネットワークインターフェースハードウェア
- ・ 不揮発性RAM内のマーチャント識別子コードナンバ
- ・ BIAに接続されるDTCシリアルポート
- ・ 磁気ストライプカードリーダー（当該分野で公知である）
- ・ ECR（電子キャッシュレジスタ）接続ポート
- ・ オプションのスマートカードリーダー（当該分野で公知である）

DPCがBIAトランザクション承認要求に対して肯定的に応答するためには2つのエンティティ、すなわち、個人とマーチャントとが識別される必要がある。

個人はバイオメトリック-PICにより識別され、マーチャントはDPCにより識別される。DPCは、BIAのVAD記録内に含まれるマーチャントコードを、RPTによりトランザクション要求に追加されたマーチャントコードとクロスチェックする。

まず、マーチャントがトランザクションの値を電子キャッシュレジスタにエンタする。次いで、個人がバイオメトリック-PICおよびアカウントインデックスコードをエンタし、その後量を確認する。RPTはその後、製品情報とマーチャントコードとをBIAに追加し、トランザクションを作成するようにBIAに指示し、そしてネットワーク接続（モデム、X.25など）を介してトランザクションをDPCに送信する。

DPCは、このメッセージを受け取ると、バイオメトリック-PICの有効性を証明し、インデックスコードを用いてアカウントナンバを獲得し、メッセージ内のマーチャントコードを、BIAの登録されたオーナーとクロスチェックする。すべてが合致した場合、DPCは交換を実行するためにクレジット／デビットトランザクションを形成して送信する。クレジット／デビットネットワークからのレスポンスは、秘密コードに追加されてトランザクションレスポンスメッセージを形成する。DPCはその後、トランザクションレスポンスメッセージをRPTに送り返す。RPTは、承認が成功したか否かを見るためにレスポンスを調べ、その後レスポンスをBIAにフォワードする。するとBIAは、個人の秘密コードを表示して、トランザクションを終了する。

RPTとDPCとの間のメッセージは、暗号化およびBIAからのMAC演算によって安全化される。MACは、RPTがメッセージの暗号化されていない部分を調べることができるが、RPTは上記部分を変更することができない。暗号化は、メッセージの暗号化された部分がRPTに開示されることを妨げる。

各小売りBIAは、マーチャントに登録されなければならない。このことは、BIA窃盗を思いとどまらせることを補助する。さらに、RPTは各メッセージにマーチャントコードを追加するため、マーチャントのBIAが異なるBIAで置換されると、DPCで行われるクロスチェックにより検出される。

ターミナル：インターネットPOS

インターネットPOS(IPT)の目的は、コンピュータを使用している個人からマーチャントへのクレジットおよびデビットの金銭的トランザクションを承認することである。この場合、個人およびマーチャントの両方がインターネット上にいる。

インターネットは、単に、マーチャント、DPC、およびIPTのすべてがリアルタイムで互いに接続できる汎用ネットワークを表すにすぎないことに留意されたい。その結果、このメカニズムは、他のいずれの汎用ネットワークとも全く同様に作用する。

IPTの構成：

- ・ BIA／PC
- ・ マイクロコンピュータ
- ・ インターネットショップソフトウェアアプリケーション
- ・ インターネット（または他のネットワーク）接続

IPTは、個人を識別することに加えて、トランザクションの相手である遠隔のマーチャントをも識別しなければならない。マーチャントはまた、DPCとIPTの両方を識別しなければならない。

インターネットショッププログラムは、購入が行われているマーチャントのホストネーム（または他の形態のネットネーム）を、マーチャントが誰であることを検証するために格納する。マーチャントはすべての合法的インターネットホストをDPCに登録しているため、このことは、DPCがマーチャントコードを、ホストネームで格納されているマーチャントコードとクロスチェックしてマーチャントが誰であることを検証することを可能にする。

まず、IPTは、インターネットを用いてマーチャントに接続する。一旦接続が確立されると、IPTはセッション鍵を生成してマーチャントに送信することにより、接続を安全化する。セッション鍵が開示されないように保護されていることを保証するために、セッション鍵は、公開鍵暗号化を用いてマーチャントの公開鍵で暗号化される。マーチャントは、暗号化されたセッション鍵を受け取ると、秘密鍵を用いてそれを復号化する。このプロセスを、公開鍵暗号化シークレット鍵交換を介して接続を安全化するという。

一旦接続されると、IPTは、マーチャントからマーチャントコード、および価格と製品との両方の情報をダウンロードする。一旦個人が購入を行う準備ができると、個人は購入したい商品を選択する。その後、個人は、BIA／PCを用いてバイオメトリックPICをエンタする。IPTはマーチャントコード、製品識別情報、および量をBIAに送信し、遠隔トランザクション承認要求を作成するようにBIAに指示する。その後、IPTは安全なチャンネルを介して要求をマーチャントに送信する。

マーチャントは、IPTがマーチャントと有するものと同一の種類の安全な接続

を介して、すなわち、公開鍵暗号化を用いて、DPCに接続して安全なセッション鍵を送信する。しかし、IPT-マーチャント接続とは異なり、マーチャント-DPCセッション鍵は、1 接続だけでなく1 日中有効である。

マーチャントはDPCに接続して、セッション鍵を用いて接続を安全化し、有効性証明のためにトランザクションをDPCにフォワードする。DPCは、バイオメトリック-PICの有効性を証明し、要求に含まれるマーチャントコードを要求内で送信されたホストネームで格納されているマーチャントコードとクロスチェックし、その後トランザクションをクレジット／デビットネットワークに送信する。一旦クレジット／デビットネットワークが応答すると、DPCは、クレジット／デビットの承認、暗号化された秘密コード、および個人のアドレスを含む応答メッセージを作成して、そのメッセージをマーチャントに送り返す。

マーチャントは一旦応答を受け取ると、応答から個人のメーリングアドレスをコピーして、承認コードを記録し、IPTに応答メッセージをフォワードする。

IPTはBIAへの応答を取り扱い、BIAは秘密コードを復号化してLCDスクリーン上に表示し、DPCが個人を認識したことを示す。IPTはまた、成功したか失敗であったかにかかわらず、トランザクションの結果を示す。

システムは概して、ネットワーク上の敵はいずれの点においてもネットワーク接続をハイジャックすることが可能であると仮定しているため、すべてのパーティはリアルタイムインタラクション中に安全な通信を有していなければならない。主な懸念は、情報の開示ではなく、メッセージの挿入または再送信である。

公開鍵暗号化のシステム全体が公開鍵用の信頼されたソースを有することに依

存している。これらの信頼されたソースは、証明オーソリティと呼ばれており、このようなソースが近い将来インターネット上で使用可能であると考える。

ターミナル：インターネットテラターミナル

インターネットテラターミナル(I T T)は、インターネット銀行トランザクションセッションの際に個人を識別するために利用される。D P C、銀行のコンピュータシステム、および個人は全てインターネットに接続している。

2つの主要タスクがある。第1の主要タスクは、I T Tからインターネット銀

行への安全な通信チャネルを提供することである。第2の主要タスクは、インターネット銀行に完璧な識別証明書を提供することである。この両方が達成されればすぐに、I T Tは、安全なインターネット銀行トランザクションセッションを提供することができる。さらに、B I Aの課題である応答検証能力は、全ての高額および/またはイレギュラーなトランザクションに対してさらなる安全性を提供するために使用される。

I T Tは、以下から構成される、すなわち

- ・ B I A (標準 P C モデル)
- ・ マイクロコンピュータ
- ・ インターネットテラー (Internet Teller) ソフトウェアアプリケーション
- ・ インターネット接続

I T Tは、個人のインターネットターミナルとして機能するマイクロコンピュータに接続されたB I A / P Cを用いて、バイオメトリック識別を承認する。

個人および銀行の両方か、D P Cによって識別され、それによって、ネットワーククリデンシャルが作成される。ネットワーククリデンシャルは、個人の識別および接続の内容（すなわち、T C P / I P ソースおよびデスティネーションポート）を含む。

D P Cは、I T TがD P Cに送る銀行のホストネームと、銀行がI T Tに送るコードとをクロスチェックすることにより銀行を識別する。

第1に、I T Tはインターネット銀行に接続し、銀行が、個人のための新しいセッションを扱うために必要とされるコンピューティングリソースを有することを確認する。銀行が十分なリソースを有する場合、銀行識別コードをI T Tに送り返す。

一旦接続されれば、I T Tは、バイオメトリックP I Cおよびアカウントインデックスコードを個人から入手することをB I Aに指示する。次にI T Tは、銀行のホストネームおよび銀行コードの両方を加える。この情報の全てを用いて、B I Aは、次に、インターネットを介してI T TがD P Cに送るネットワーククリデンシャルリクエストメッセージを作成するように依頼される。

D P Cがこのメッセージを受け取れば、D P Cは、バイオメトリックP I Cの有効性を証明し、インデックスコードを用いてアカウントナンバーを入手し、メッセージからの銀行コードが、遠隔マーチャントデータベースにおける銀行のホストネームの下に格納された銀行コードと一致するかどうかを確認する。D P Cはまた、インデックスコードによって返されたアカウントナンバーが、銀行のものであるかの確認を行うためにチェックする。すべてがチェックされれば、次に、D P Cは、個人のアカウント識別、その日の時間、および銀行コードを用いてネットワーククリデンシャルを作成する。D P Cは、公開鍵暗号化およびD P Cの秘密鍵を用いて、このクリデンシャルに署名する。D P Cは、銀行の公開鍵および個人の秘密コードを取り出し、そしてクリデンシャルを用いてネットワーククリデンシャルレスポンスメッセージを形成する。レスポンスメッセージは、B I Aレスポンス鍵を用いて暗号化され、その後、I T Tに送り返される。

I T Tがそのレスポンスを受け取る時、I T Tは、B I Aにレスポンスメッセージを渡す。B I Aは、復号化を行い、次に、個人の秘密コードをL C Dスクリーン上に表示する。銀行の公開鍵は、公開鍵レジスタに格納される。2つのランダムセッション鍵は、B I Aによって生成される。共用セッション鍵と呼ばれる第1の鍵は、平文でI T Tに明らかにされる。I T Tは、この共用セッション鍵を用いることにより、銀行との接続を確実にする。

秘密セッション鍵と呼ばれる他方のセッション鍵は、I T Tと共用されない。これは、B I Aのチャレンジャーレスポンスメカニズムのために用いられ、このメカニズムは、銀行が、（信用できない）I T Tに関与することなしに、個人から直接の非ルーチントランザクションに対する特定の有効性の証明を得ることを可能にする。

共用セッション鍵を受け取った後、I T Tは、B I Aに、セッション鍵とネットワーククリデンシャルの両方を含み、銀行の公開鍵を用いて全て暗号化される安全接続要求メッセージを作成するように依頼する。I T Tは次に、安全接続要求メッセージを銀行に送る。

銀行は、リクエストメッセージを受け取ると、銀行自身の秘密鍵を用いてメッ

セージを復号化する。その後、D P Cの公開鍵を用いて実際のネットワーククリデンシャルを復号化する。ネットワーククリデンシャルが有効で、期限が切れていなければ（クリデンシャルは、ある数分後に時間切れとなる）、その個人は承認され、安全を確実にするために使用されるセッション鍵を用いて、会話が継続する。

個人が、非ルーチンまたは高価値のトランザクションを行う場合、銀行は、さらなる安全のために個人がこれらのトランザクションの有効性の証明をすることを求めることを所望し得る。そうするためには、銀行は、秘密セッション鍵を用いて暗号化されたチャレンジャーレスポンスメッセージをI T Tに送り、I T Tは、そのチャレンジャーレスポンスメッセージをB I Aにフォワードする。B I Aは、メッセージを復号化し、チャレンジ（通常、「\$2031.23をリック・アダムスに振替O K？」の形態）を表示し、個人がO Kボタンを打つことにより有効性の証明をすれば、B I Aは秘密セッション鍵を用いてレスポンスを再び暗号化し、そのメッセージをI T Tに送り、I T Tは、そのメッセージを銀行にフォワードし、トランザクションの有効性を証明する。

このシステムは、クリデンシャルを提供し、かつI T Tと銀行との間の通信を確実とするために公開鍵暗号系を利用する。

このメカニズムが正しく機能するためには、銀行はD P Cの公開鍵を知っていなければならない。D P Cは、銀行の公開鍵を知っていなければならない。システムの安全のためには、両方のパーティが、承認されていない改変から、互いの公開鍵を安全に管理することが重要である。公開鍵は、誰によっても読むことが可能であるが、ただ、誰によっても改変可能となることはできないことに注意されたい。もちろん、どのようなセッションまたは秘密鍵は、観察から安全に管理されなければならない。これらの秘密鍵は、セッションの終了後に破壊されなければならない。

非ルーチントランザクションのための余分な確認ステップは、ウイルス、ハッカー、および個人の無知が原因で、インターネット上でパーソナルコンピュータアプリケーションを保護することが比較的困難であるので、必要である。銀行は

、ユーティリティ会社、主なクレジットカードのベンダーなどのよく知られた機関への金銭振替のみを包含するように、I T Tに利用可能なルーチン金銭振替をおそらく限定すべきである。

ターミナル：電子署名

電子署名ターミナル（E S T）は、電子文書に関して偽造不可能である電子署名を作成するために個人によって使用される。E S Tにより、個人が電子文書に署名すること、または、そのような文書にすでにある電子署名を検証することが可能となる。

E S Tの構成：

- ・ B I A／P C
- ・ マイクロコンピュータ
- ・ メッセージダイジェストエンコーダアルゴリズム
- ・ モデム、X. 25 接続、またはインターネット接続
- ・ 電子署名ソフトウェアアプリケーション

E S Tは、電子署名ソフトウェアアプリケーションによって制御されたイベントに関して、マイクロコンピュータに取り付けられたB I A／P Cを使用する。

ある種の公開／秘密鍵をかけられたトークンを使用することなしにデジタル署名を作成するためには、3つの事が行われなければならない。第1に、署名される文書は、固有に識別されなければならない、その日の時刻が記録されなければならない、署名を行っている個人が識別されなければならない。これにより、文書、個人、および時刻がリンクされ、一意のタイムスタンプされた電子署名が作成される。

第1に、署名される文書は、メッセージダイジェストコードを生成するメッセージダイジェストコード化アルゴリズムによって処理される。このようなアルゴ

リズムの1つに、当該分野でよく知られている、R S AによるM D 5アルゴリズムがある。本来、メッセージダイジェストアルゴリズムは、同じメッセージダイジェストコードを生成する別の文書を提示することがほとんど不可能となるように特別に設計されている。

次に、個人は、B I Aを用いてバイオメトリックP I Cを入力し、メッセージダイジェストコードはB I Aに渡され、文書名が加えられ、その結果生じるデジタル署名リクエストメッセージが、識別および保存のためにD P Cに送られる。

D P Cはリクエストを受け取り、バイオメトリック識別チェックを行い、個人が一旦検証されれば、メッセージダイジェストコード化と、個人のバイオメトリックアカウントナンバーと、その日のその時の時刻と、文書名と、署名を集めたB I Aの識別を収集し、それら全てを電子署名データベース（E S D）に格納する。D P Cはその後、E S Dレコードナンバー、日付、時刻、および署名者の名前から成る署名コードテキストストリングを作成し、この署名コードを個人の秘密コードと共に、E S Tに送り返す。

電子署名をチェックするために、文書は、MD 5アルゴリズム（当該分野で公知）を通して送られ、その結果生じる値は、電子署名コードと一緒に、B I Aおよびリクエストしている個人のバイオメトリックP I Cに与えられ、メッセージはD P Cに送られる。D P Cは、各署名の有効性チェックを行い、適切に応答する。

B I Aは、電子署名に関係するどのようなデータも暗号化しないので、特定のMD 5の値と共に、文書タイトルが、平文で送られる。署名の有効性の証明に対しても、同じ状況が当てはまる。

従って、署名が偽造され得ない一方で、詳細のいくつか（文書名を含む）は、妨害に弱い。

ターミナル：証明された電子メールターミナル

証明電子メールターミナル（C E T）の目的は、個人に、送り手の識別、受け取りおよび受け手両方の検証を提供し、メッセージ配送の秘密性を確実にしながら、電子メッセージをシステム内の他の個人に送る方法を提供することである。

C E Tは、B I A／P Cを用いることにより、送り手および受け手の両方を識別する。安全は、メッセージを暗号化し、その後、アップロードの間に、送り手のB I Aを用いてメッセージ鍵を暗号化し、次に、ダウンロードの間に、受け手のB I Aを用いてメッセージ鍵を復号化する。

送信者および受け手のCETの構成：

- ・BIA
- ・マイクロコンピューター
- ・モデム、X.25接続、またはインターネット接続
- ・電子メールを受け取る能力
- ・証明された電子メールアプリケーション

実際、CETは、電子メールアプリケーションと、証明された電子メールを送信および受信するためのバイオメトリックPIC承認を生じさせるためにBIAを呼び出すネットワーク接続とを有するマイクロコンピューターである。

メッセージの配送を保証するために、送り手および受け手は共に、識別されなければならない。

送り手は、メッセージをDPCにアップロードするときに、バイオメトリックPICを用いて、自分自身を識別する。送り手が文書を送ることを望む各受け手は、バイオメトリックアカウント識別ナンバーまたはファックス番号のどちらか一方、およびエクステンションによって識別される。受け手が、メッセージをダウンロードするためには、自分のバイオメトリックPICを用いて自分自身を識別する。この手順は、指名電話に似ている。

メッセージの配送は、個人が、文書またはメッセージをアップロードし、バイオメトリックPICを用いて自分自身を識別することで始まる。個人は、その後、文書名を検証し、電子メールメッセージは、暗号化され、アップロードされる。

メッセージが一旦アップロードされれば、送り手は、各受け手に対する文書の現在の配送ステータスをリクエストするために使用され得るメッセージ識別コードを受け取る。

DPCは、電子メールメッセージを各受け手に送り、証明されたメッセージが到着した時に、受け手に知らせる。

一旦受け手が告知を受け取れば、受け手は、都合のよい時に、バイオメトリックPICを入手し、DPCに有効性の証明をさせることにより、メッセージまた

はメッセージ群を受けるまたは拒否することのどちらかを選択し得る。

一旦、全ての受け手にうまく送信されれば、所定の期間後、通常24時間後、文書は取り除かれる。文書を、メッセージが送られた全ての個人の表示と共にアーカイブ化することを望む個人は、メッセージの削除の前に、メッセージアーカイブリクエストを入力し得る。

送信の安全な面をもたらすために、文書は、途中で公開されることから保護される。CETは、BIAによって生成される56ビットメッセージ鍵を用いることにより、これを達成する。BIAは、バイオメトリックPICの一部としてメッセージ鍵を暗号化する責任を引き受けるので、暗号化鍵は、安全にDPCに送られる。

個人がメッセージをダウンロードする時に、メッセージ鍵は、秘密コードとともに暗号化されて送られることにより、受け手がメッセージを復号化することが可能となる。全員が同じメッセージを受け取るので、全ての受け手がこのメッセージ鍵を持つようにしてもよいことに注目されたい。

ITTの場合と同じように、一旦個人が文書名の有効性を証明すれば、改変されたCETが所望のどのような文書も送ることができるので、個人は、CETアプリケーションソフトウェアを不正な改変から保護するように注意しなければならない。

ターミナル：安全ファックスターミナル

安全ファックスターミナル（SFT）の目的は、個人に、送り手の識別、受け取りおよび受け手両方の検証を提供し、メッセージ配送の秘密性を確実にしながら、ファックスメッセージをシステム内の他の個人に配送する方法を提供することである。

各SFTは、送り手および受け手の両方を識別するために、集積型BIA／ケーブルテレビを使用する。通信セキュリティは、暗号化を通して達成される。

送信者および受け手両方のSFTの構成：

- ・ BIA／ケーブルテレビ
- ・ ファックスマシン

・オプションのISDNモデム

SFTは、モデムを介してDPCに接続されたファックスマシンである。このシステムは、ファックスを、証明された電子メールの単なる別のタイプのものとして扱う。

安全なファックスに関して、セキュリティのいくつかの異なるレベルが存在するが、最も安全なバージョンにおいては、送り手および全ての受け手の身元が検証される。

送り手は、メッセージをDPCに送る際に、バイオメトリックPICおよびタイトルインデックスコードを用いて、自分自身を識別する。ファックスを受け取るためには、リストされた各受け手が、バイオメトリックPICおよびタイトルインデックスコードを再び用いて自分自身を識別する。

さらに、受け取りサイトは電話番号によって識別される。この電話番号は、DPCを用いて登録される。安全な秘密のファックスに関しては、各受け手が、電話番号およびエクステンションを用いて識別される。

SFTが送ることのできるファックスには5つの基本的なタイプがある。

I. 非安全性ファックス

安全にされていないファックスは、標準のファックスに等しい。送り手は、受け手のサイトの電話番号を入力し、ファックスを送る。この場合、送り手は、識別されないまま、ファックスは、正しい受け手に配送されることを期待して、与えられた電話番号に送られる。SFTは、そのような全ての安全にされていないファックスのトップラインに、「非安全性」（「UNSECURED」）であると目立つように印をつける。非SFTファックスマシンから受け取られた全てのファックスは、常に、非安全性であると印がつけられている。

II. 送り手安全ファックス

送り手安全ファックスにおいては、送り手は、ファックスマシンの「送り手安全」モードを選択し、タイトルインデックスコードに続いてバイオメトリックPICを入力する。次に、ファックスマシンは、DPCに接続し、バイオメトリックPIC情報を送る。一旦DPCが個人の同一性を検証すれば、個人は次に文書

をファックススキャナに送り込むことによりファックスを送る。この場合、ファックスは、実際に、ファックスをデジタル形式で格納するD P Cに送られる。一旦全部のファックスがD P Cに到着すれば、D P Cは、各宛先にファックスを送ることを開始し、各ページは、各ページのトップに「送り手安全」（「SENDER-SECURED」）の大見出しとともに、名前、タイトル、および送り手の会社をラベル表示する。

I I I. 安全ファックス

安全ファックスにおいては、送り手は、ファックスマシンの「安全」モードを選択し、タイトルインデックスコードに続いてバイオメトリックP I Cを入力し、その後、受け手の電話番号を入力する。一旦システムが送り手の身元および各受け手の電話番号を検証すれば、その後、個人は、文書をファックススキャナに送り込むことによりファックスを送る。次に、ファックスは、ファックスをデジタル形式に格納するD P Cに送られる。一旦全部のファックスがD P Cに届けば、D P Cは、未完の安全ファックス、送り手のタイトルおよび身元、そして、トラッキングコードと共に待機中のページ数を示す小さなカバーページを宛先に送る。このトラッキングコードは、自動的に受け手のファックスマシンのメモリに入力される。

ファックスを取り出すためには、受け手の会社の従業員が、ファックスマシンの「ファックス取り出し」ボタンを選択し、トラッキングコードを用いることにより、未完のどのファックスを取り出すかを選択し、次に、バイオメトリックP I Cを入力し得る。ファックスが不要な場合は、個人は、「ファックス拒絶」ボタンを押し得るが、それでもやはり、そうするためには、システムに対して自分自身の識別を行わなければならない。一旦会社のメンバーとして有効性を証明されれば、次に、ファックスは受け手のファックスマシンにダウンロードされる。各ページは、各ページのトップに、送り手の身元およびタイトル情報と共に、

「安全」（「SECURED」）の文字を有する。

I V. 安全性秘匿ファックス

安全性秘匿ファックスにおいては、送り手は、ファックスマシンの「安全性秘

匿」モードを選択し、タイトルおよびインデックスコードに続いてバイオメトリックP I Cを入力し、次に、各受け手の電話番号およびシステムエクステンションを入力する。一旦D P Cが送り手の身元および各受け手の電話番号およびエクステンションを検証すれば、個人は次に、ファックススキャナに文書を送り込むことにより、ファックスを送る。ファックスは、ファックスをデジタル形式で格納するD P Cに送られる。一旦全部のファックスがD P Cに届けば、D P Cは、未完の安全性秘匿ファックス、送り手のタイトルおよび身元、受け手のタイトルおよび身元、そして、トラッキングコードと共に、待機中のページ数を示す小さなカバーページを各宛先に送る。このトラッキングコードは、自動的に受け手のファックスのメモリに入力される。しかし、ファックスを取り出すことのできる唯一の個人は、エクステンションコードが示されている個人である。

この個人は、「ファックス取り出し」ボタンを選択し、取り出すべき未完のファックスを選択し、次にバイオメトリックP I Cを入力する。一旦受け手としての有効性を証明されれば、ファックスは、次に受け手のファックスマシンにダウンロードされる。各ページは、各ページのトップに、送り手のタイトルおよび身元情報と共に「安全性秘匿」（「SECURED-CONFIDENTIAL」）の文字を有する。

V. 安全性秘匿契約ファックス

このファックスは、受け手に対するファックスの実際の配送に関しては、ファックスが、安全性秘匿の代わりに「契約」とタイトルを付けられることを除いては、安全性秘匿ファックスと同様に処理される。さらに、D P Cは、自動的に契約ファックスをアーカイブ化する。どのような受け手も、契約ファックスの受け取りに続くS F Tによって、契約を受けるまたは拒絶し得る。従って、オプションで、D P Cは電子書記の役割を果たす。

システムに送られ、その後、受け手にフォワードされるどのようなファックスも、送信ファックスマシンをタイアップすることなしに、いかなる数の受け手にも送られ得る。さらに、送られたいかなるファックスのトラッキングナンバーが、ファックスマシンのメモリに入力され、継続中のいかなるファックスのステータスレポートが、「ステータス」ボタンを選択し、その後、特定のファックス未

完トラッキングコードを選択することにより、送信マシンにおいて生成され得る。D P Cは、各受け手に対する送信状態を詳述し、送信ファックスマシンに直ちに送られるレポートを発行する。

いかなる安全または安全性秘匿ファックスに関して、送り手または受け手の1人のどちらか一方が、今後の参考のために、ファックスを（誰がファックスを送り、誰がファックスを受け取ったかに関する詳細と共に）アーカイブ化するというオプションが存在する。このために、いかなる安全ファックスも、成功した配達の後、ある期間（すなわち24時間）保持される。アーカイブトラッキングコードは、アーカイブのリクエストがあればいつでも個人に戻される。このアーカイブコードは、ファックスと、システムにアーカイブ化されたファックスステータスレポートとの取り出しに使用される。

アーカイブされたファックスは、ある期間（すなわち24時間）の後、読み取り専用の二次記憶装置に配置される。アーカイブ化されたファックスを取り出すことは、人の介入を必要とし、遂行に24時間までかかり得る。

S F Tシステムは、受け手が送り手の身元を確かめるために懸命に働き、受け手が実際に文書の受け取りを了承したことを送り手が確かめるために、同じ様に懸命に働く。

送り手と受け手との間の通信の妨害に対して保護を行うために、ファックスターミナルは、B I Aによって提供されるメッセージ鍵機能を用いてファックスを暗号化する。B I Aは、バイオメトリックP I Cの1部としてメッセージ鍵を暗号化する責任を取るので、暗号化鍵は、安全にD P Cに送られる。

個人が、いかなるタイプの安全ファックスを受け取る際には、メッセージ鍵は、秘密コードとともに暗号化されて送られることにより、受け手がメッセージを復号化することが可能となる。全員が同じメッセージを受け取るので、全ての受け手がこのメッセージ鍵を有するようにしてもよいことに注目されたい。

ターミナル：バイオメトリック登録ターミナル

バイオメトリック登録ターミナル（B R T）の目的は、バイオメトリックP I C、メーリングアドレス、秘密コード、電子メールアドレス、タイトルと電子メ

ッセージおよびファックスの送信および受信に用いられるタイトルインデックスコードのリスト、および、財政的資産アカウントおよびアクセスでき得るアカウントインデックスコードのリストを含む新しい個人の登録をすべて、バイオメトリックP I Cを用いて行うことである。

登録プロセスの目的は、情報の有効性が証明され得る責任機関の場所で、個人から個人情報を得ることである。これは、リテイル銀行店および企業の人事部を含むが、それらに限定されるものではない。参加している責任機関の各々は、登録を行うことを承認された従業員のグループによって使用される1つのB R Tを有する。各従業員は、登録された各個人に対して責任がある。

B R Tの構成：

- ・マイクロコンピューター、およびスクリーン、キーボード、マウス
- ・B I A／R e g
- ・9．6 k bモデム／X．2 5ネットワーク接続（当該分野で公知）
- ・バイオメトリック登録ソフトウェアアプリケーション

B R Tは、バイオメトリック入力に対して、取り付けられたB I A／R e gを用い、9．6 k bモデムまたはX．2 5ネットワーク接続（当該分野で公知）によってシステムに接続される。バイオメトリック登録ターミナルは、リテイル銀行店などの物理的に安全な場所に位置する。

D P CがB I A／R e g登録リクエストに確実に応答するためには、3つのエンティティ：登録する従業員、機関およびB I A／R e gが識別される必要がある。従業員は、個人をその機関に登録するためには承認されていなければならない。

機関およびB I Aは、B I Aの所有者とB R Tによって設定された機関コードとをクロスチェックすることにより識別される。従業員は、登録アプリケーションを開始させる際に自分のバイオメトリックP I Cを入力することにより、システムに対して自分を識別させる。

機関は、個人をシステムに登録する前に、標準顧客識別プロシージャ（署名カード、従業員記録、個人情報など）を用いる。登録する個人は、随意にアカウン

トから金銭を転送および／または電子メッセージを会社の名前を使って送る権限を与えられるので、機関にとって個人の同一性をできる限り根気強く検証することが重要である。

登録する間に、個人は第一次および二次のバイオメトリックの両方を入力する。個人は、両方の人差し指を使用しなければならず、個人に人差し指がない場合には、隣りの親指が使用され得る。特定の指が使われることを要求することにより、以前の詐欺のチェックを行うことが可能となる。

個人は、第1の指および第2の指を選択することを奨励され、DPC同一性チェックの間、第1の指が優先されるので、個人は、第1の指として、最もよく使う指を示すべきである。もちろん、DPCは、そうすることが重要であると判明すれば、操作に基づく第1および第2のバイオメトリックスの指定を変更することを選択することも可能である。

バイオメトリックコード化プロセスの一部として、BIA/Rは、個人が「良い指紋」を入力したかどうかを決定する。研磨剤または酸を用いて働く個人など、仕事が、結果として偶発的な指紋の除去につながる個人もいることに注意されたい。残念なことに、これらの個人は、このシステムを使用することができない。彼らは、プロセスのこの段階で検知され、関与できないことを告げられる。

個人は、システムの中心データベースによって提供される一連のPICオプションから、4から12桁からなるPICを選択する。しかし、PICは、システムによって有効性を証明されなければならない。これは、2つのチェックを伴い、1つは、（PICは、バイオメトリック比較アルゴリズムによってチェックされる個人の数を減らすために使用されるので）同じPICを用いる他の個人の数が多すぎないこと、そして、生物測定的にいて、登録されている個人が、同じPICグループの他の個人とあまりにも「近く」ないことである。どちらかが起こった場合、登録は拒否され、エラーメッセージがBRTに戻され、個人は異なるPICをリクエストすることを指示される。このシステムは、個人がPIC下の

システムにおいて記録をすでに有することを示す「同一性一致」エラー状態を、

任意に返答し得る。

OのPICにより、システムがPICを個人に割り当てることが可能となる。

個人は、ワードまたはフレーズからなる秘匿性秘密コードを作成する。個人がそれを作成することを望まない場合は、秘密コードが、ターミナルによってランダムに作成される。

個人は、その金融資産コードリストをアレンジすることもできる。このリストには、どのアカウントインデックスコードがどのアカウント（即ち、1. 借方、2. 貸方、3. 緊急借方、等）を指しているのかが記されている。これは、登録機関が銀行であり、且つ、アカウントがその特定の銀行機関によって所有されている場合にのみ行われ得る。

登録後であっても、以前の詐欺のチェックが完了するまでは、システムを使用して実際に処理を行うことはできない。一般に、これにかかるのは数分であるが、ハイロードの時間帯には最高数時間かかる。システムが以前の詐欺の事例が全くないことを認めるまでは、その個人のアカウントはアクティベートされない。

個人が、それまでに1回でもシステムを詐取したことがあると認められた場合、DPCは、その犯罪者について、全データベース強制バイオメトリックデータベースサーチ(database-wide involuntary biometric database search)を開始する。これらの中のいくつかは毎晩行われ、軽いアクティビティ条件の間に(during conditions of light activity)時間のかかる処理を行うことによって、システムから特に指名手配されている個人がデータベースから吹き飛ばされる。

ターミナル：顧客サービス

顧客サービスターミナル(CST)の目的は、内部のDPCサポート職員に、システムデータベースの様々な局面へのアクセスを提供することである。サポート係は、システムに関するトラブルをかかえる個人、発行者、機関、およびマーチャントの問い合わせに答えなければならない。

CSTの構成：

- ・マイクロコンピュータ
- ・BIA／Int

- ・イーサネット／トークンリング／FDDIネットワークインターフェース
- ・データベース検査および改変用アプリケーション

各CSTは、トークンリング、イーサネット、ファイバ（FDDI）等の高速ローカルエリアネットワーク接続を介してシステムに接続される。各CSTは、データベースのそれぞれに対して照会を行って、その照会結果を表示することができる。但し、CSTは個々のターミナルユーザの特権に基づいたフィールドおよび記録だけを表示する。例えば、標準的な(standard)顧客サービス従業員は、そのBIAを現在どのマーチャントあるいは個人が所有しているのかを見ることはできるが、所与のBIAのVDB記録の暗号化コードを見ることはできない。

CSTによってデータベースへのアクセスが許可されるには、その個人およびそのBIAがシステムによって識別されなければならない。さらに、データベースがアクセスを適切に制限するためには、その個人の特権レベルも決定されなければならない。

CSTを使用する個人は、そのバイオメトリックPICを入力して識別子を提供することによってセッションを開始する。BIAは、認識リクエストメッセージを作成して、それを、検証のためにDPCに送信する。システムがその個人を検証すると、CSTアプリケーションは、予め指定されたその個人のDPC特権レベルによって制限されるものの、通常処理を行うことができるようになる。

故意に、あるいは知らない間にウィルスが導入される等、いかなる方法によってもデータベースアプリケーションが改変されないことが重要である。この目的のために、個々のCSTには、フロッピードライブや他の取り外し可能な媒体が全くない。さらに、実行可能なデータベースアプリケーションへの読出しアクセスは、知る必要性のある者だけにきびしく限定される。

不正な改変や漏洩(disclosure)からCSTおよびデータベース間の通信を保護するために、CSTは、CSTおよびデータベース間のトラフィックを全て暗号

化する。これを行うために、CSTはセッション鍵を生成する。この鍵は、システムとのログインセッションの間にサーバに送信される。このセッション鍵を用いて、期間中に生じるDPCとの全通信の暗号化および復号化を行う。

通信が安全であり、データベースアプリケーションの改変が全くないと仮定した上で、D P Cは、C S Tを使用している個人にはアクセス不可能なD P CデータフィールドがC S Tデータベースアプリケーションに送信されることがないようにする。同様に、どの時点においても、いかなるC S T職員にも、個人のバイオメトリック情報を改変するためのアクセスあるいは許可は与えられない。

D P Cとサポートセンタとは同じ場所にあってもよいし、あるいは、C S T周辺のセキュリティはかなり嚴重であるので、サポートセンタを分けて独立させてもよい。

ターミナル：発行者ターミナル

発行者ターミナルの目的は、発行銀行(issuing banks)の従業員が、D P Cに対するバッチ資産アカウント改変処理の入力を安全且つ識別可能に行うことができるようにすることである。

I Tの構成：

- ・マイクロコンピュータ
- ・モデム、X. 25ネットワーク、あるいはシステムへのインターネット接続
- ・B I A／I s s
- ・銀行の内部ネットワークへのネットワーク接続

発行者ターミナルは発行者B I Aを用いて、金融資産情報に関する大量の追加および削除を承認する。

この処理においては、銀行が識別されなければならず、適正に承認された銀行の従業員が識別されなければならず、また、資産アカウントの追加または削除を行っている個人が全て識別されなければならない。

銀行は、銀行のアカウント(口座)を資産アカウントリストに追加しようとして

いる個人を識別する役割を有する。バイオメトリック登録の場合と同様に、これは、署名カードおよび個人情報を用いて銀行によって行われる。I Tによって入力された発行者コードとB I A／I s sのV A D記録内に登録されている発行者コードとをクロスチェックすることによって、D P Cは銀行を識別する。バイオメトリックP I Cを用いて、そのバッチを実際に入力している銀行の従業員を識

別する。

金融資産アカウントを追加する際、個人は、追加するアカウント(口座)と一緒に、その個人のバイオメトリック識別番号を銀行に与える(この識別番号は、初めのバイオメトリック登録ステップの際に個人に与えられる)。個人が適切に識別された後、この識別コードおよびアカウントリストをITにフォワードして、それ以降のバッチのシステムへの入力を行う。

銀行が適切であると認める場合はいつでも、銀行の承認された個人は、ITに命令を与えて、DPCへのバッチ化されたアカウント追加/削除をアップロードさせる。これを行うために、承認された個人はバイオメトリックPICを入力し、ITはセッション鍵の追加および銀行の発行者コードの追加を行い、これにより、BIA/Issは、発行者バッチリクエストメッセージを作成し、その後、ITはこれをDPCにフォワードする。ITは、メッセージコードを用いてそのバッチを暗号化した後、その送信も行う。

システムは、発行者バッチリクエストを受信すると、そのBIAがBIA/Issであること、そのBIA/Issが発行者コードによって要求されている銀行に登録されていること、ならびに、そのバイオメトリックPICにおいて識別される個人がその銀行についてDPCにバッチリクエストを入力することを許可されていることを確認する。そうである場合、DPCは、必要に応じてエラーの記録をとりながら、全てのリクエストを処理する。これが終了すると、DPCは、処理中に生じた全てのエラーを有する暗号化されたバッチと一緒に、個人の秘密コードを返す。

このシステムのセキュリティにとって、このトランザクションのセキュリティは決定的である。詐欺行為をしようとする悪意があれば、他人のアカウントを自分のバイオメトリック識別コードに追加する方法を見つけるだけで、思いのまま

に詐欺行為を行うことができるようになる。最終的には、その犯罪者はとらえられて、データベースから一掃されるのだが、それは、その犯罪者が他人のアカウントを空にしてからのことである。

銀行とBIA/Issとをクロスチェックすることは、ITおよびBI

Aが共に偽の追加／削除メッセージをD P Cに入力するようにしなければならないことを意味する。従って、銀行は、I Tが物理的に安全であり、且つそのアクセスが承認された個人だけに許可されていることを確実にしなければならない。

ターミナル：自動預金支払機(Automated Teller Machinery)

バイオメトリックA T Mの目的は、インターバンクカード(interbank card)を用いる必要なく、現金へのアクセスおよび他のA T M機能を個人に提供することである。これは、バイオメトリックP I Cおよびアカウントインデックスコードを入力して、銀行口座番号を取り出すことによって行われる。システムのユーザにとって、これは、インターバンクカード（当該分野では公知）＋口座を識別して個人を承認するための方法としてのP I Cメカニズムにとって代わるものである。全てのA T Mが依然としてインターバンクカードを受けつけるものと仮定する。

A T Mの構成：

- ・標準的なA T M
- ・一体型B I A／A T M（スキャナのみ）
- ・D P Cへの接続

バイオメトリックA T Mは、一体型B I A／A T Mを用いて、個人を識別するとともにその個人がバイオメトリックP I Cおよびアカウントインデックスを用いて金融資産にアクセスできるようにする。B I A／A T MはA T M内に設置され、P I Cおよびアカウントインデックスコードの入力用には、既存のA T MのP I Cパッドを利用する。A T Mは、X. 25あるいはモデムを用いてシステムに接続される。

B I A／A T Mは、現存のA T Mネットワークとの一体化ができるだけ簡単になるように構成される。D P CがB I A／A T Mアカウントリクエストに適切に応答するためには、次のエンティティが識別される必要がある：個人、銀行およびB I A／A T M。

A T Mの格納銀行コードとB I A／A T Mの銀行コードとをクロスチェックすることによって、銀行が識別される。B I A／A T Mは、V A D内におけるB I

A/A T Mの特定が成功することによって識別され、個人は、標準的なバイオメトリックP I Cによって識別される。

A T Mにアクセスするために、個人は、アカウントインデックスコードと共に、バイオメトリックP I CをB I Aに入力する。B I Aは、アカウントアクセスリクエストメッセージを作成し、このアカウントアクセスリクエストメッセージはその後A T MによってD P Cに送信される。D P Cは、緊急アカウントインデックスコードとともに、バイオメトリックP I Cの有効性を証明し、その後、得られた資産アカウント番号を秘密コードと一緒にA T Mに送り返す。

A T Mは、B I Aにレスポンスを復号化するように要求し、その後、A T Mのディスプレイスクリーン上に秘密コードを表示する。また、A T Mはレスポンスを検査して、その個人が標準的なアカウントアクセスを行っているのか、それとも、「脅迫(duress)」アカウントアクセスを行っているのかを確認する。脅迫アカウントアクセスであることが分かると、A T Mは、その個人が利用可能である金額に関する偽あるいは誤解させるような情報を提供してもよい。この動作の詳細はA T Mによって異なる。但し、いかなるA T Mも、脅迫トランザクション(duress transaction)が進行中であることをその個人に示すことはない。

A T MおよびD P C間のメッセージの安全性は、暗号化およびB I AからのM A C計算によって保たれる。M A Cは、A T Mが検知されずにメッセージのコンテンツを変更することはできないことを意味し、暗号化はそのメッセージの暗号化された部分の漏洩を防ぐ。

B I A/A T Mには、L C DやP I Cパッドが付いていないので、A T Mには、あらゆるテキストプロンプトを提供して、その個人からの入力を全て集めることが要求される。これは、B I Aによってこの処理を行う場合に比べて比較的安全

でないが、一般にA T Mは物理的に頑丈であるので、おそらく問題にはならないとされるであろう。

偽のスクリーンは、不正確になるように意図的に予め決められたデータの表示であるので、脅迫者が、ある個人の金融資産についての正確なデータを不法に入

手することはない。

ターミナル：電話POSターミナル

電話POSターミナル（PPT）の目的は、特別装備の電話を用いてマーチャントからの購入を行う個人からの貸方あるいは借方金融トランザクションを承認することである。

PPTの構成：

- ・ B I A / c a t v
- ・ 高速接続デジタルモデム [VoiceView特許（当該分野では公知）を参照]
- ・ 電話（キーパッド、受話器、マイク）
- ・ マイクロコンピュータ
- ・ DSP（デジタル信号プロセッサ）
- ・ 標準的な電話線

PPTは、コードレス電話、セルラー電話、あるいは標準的な電話に接続され一体化されたB I A / c a t vを用いて、バイオメトリック識別子を受け付ける。

DPCがトランザクションを承認するためには、個人およびマーチャントの両者を識別しなければならない。個人を識別するために、バイオメトリックPIC識別が用いられる。

電話注文マーチャントを識別するために、マーチャントと、個人がかけるマーチャントの電話番号の全てをDPCに登録する。従って、個人は、承認を入力する際に、その個人がかけた電話番号も入力する。その後、この電話番号を、マーチャントの電話番号リストとクロスチェックする。

個人は、紙のカatalog、新聞、雑誌、あるいは他の基本的な印刷媒体メカニズ

ムを用いて商品を販売しているマーチャントに電話をかける。PPTは、電話音声ラインを共有する専用モデムを用いて、マーチャントとデジタル情報を交換する。

個人が電話をかける度に、個人が購入を決定した場合のために、PPTは、ユーザによって押された電話番号の記録をとる。DSPを用いて、発信音、呼出し

音(ring)、接続(connection)等を検知し、これにより、内線、あるいは電話メッセージシステムの案内等と区別して、入力された実際の電話番号が何であったのかを知る。

マーチャントに電話がかかると、そのマーチャントの販売員は、商品、価格、およびマーチャントコードを含む関連する情報を全てPPTにデジタル方式でダウンロードする。使用中、モデムはスピーカを切る(disconnect)ことに留意されたい。

商品情報がダウンロードされると、その後、PPTは個人にプロンプトを出してバイオメトリックPIC、アカウントインデックスコードを促し、その後、個人に購入金額の有効性を証明するように要求する。その後、電話番号およびマーチャントコードを追加して、メッセージを暗号化する。高速接続モデムを再び用いて、マーチャントに承認情報を送信する。

マーチャントは、承認情報を受信すると、価格および商品情報が正しいことを検証し、その後、インターネットあるいは他の汎用ネットワークを用いた安全な通信チャネルを使って、トランザクションをDPCにフォワードする。公開鍵暗号化および秘密鍵交換を用いて、DPCへの接続の安全性が保たれる。

電話承認の受信および復号化の際に、DPCはマーチャントコードに対してその電話番号をチェックし、そのバイオメトリックPICの有効性を証明し、その後、トランザクションを承認のために貸方／借方ネットワークに送信する。承認が成功すれば、DPCは購入者のアドレスをレスポンスメッセージに添付し、そのレスポンスをマーチャントに送信する。

マーチャントは、DPCからレスポンスを受信し、その宛先をコピーし、そして、高速接続モデムを用いた短時間のセッションによってメッセージを再び個人にフォワードする。IPTへの送信が完了すると、チャイムが鳴り、モデムを切

断し、個人の秘密コード(BIAによって復号化)をLCDスクリーン上に表示する。マーチャントの販売代理人は、個人の宛先が有効であることを確認し、有効であれば電話を切ってトランザクションを完了する。

ターミナル：ケーブルTVPOS

C A T V販売時点情報管理ターミナル（C P T）の目的は、テレビ受信機（または「T V」）の前にいる個人から、テレビ放送で商品を紹介しているマーチャントへの貸方または借方財政的トランザクションを承認することである。

C P Tの構成：

- ・ B I A / catv
- ・ 集積型 B I A / catvを有するテレビのリモコン
- ・ ケーブル T V デジタル信号デコーダ
- ・ ケーブル T V リモコン読み取り装置
- ・ オンスクリーン表示メカニズム
- ・ ケーブル T V 広帯域双方向通信チャンネルへのアクセス

C P Tは、テレビのリモコンデバイスに組み込まれた B I A / catvを用いて、バイオメトリック識別を受け取る。リモコンは、それ自体が広帯域ケーブルテレビネットワークと通信するテレビのトップボックスと通信する。ターミナルは、B I A と通信するテレビ遠隔ロジックおよびケーブル広帯域ネットワークで通信するテレビのトップボックスを含む。

このトランザクションにおいて、トランザクションを実行するためには、マーチャントおよび個人は共に識別されなければならない。個人は、バイオメトリック P I C によって識別される。マーチャントは、製品がテレビ放送で見せられる時に C A T V 放送局によって作成されるマーチャントクリデンシャルによって識別される。各製品の放送は、マーチャントコード、時刻、持続期間、および公開鍵暗号化と C A T V ネットワーク放送局の秘密鍵とを用いて署名される価格で構成されているマーチャント製品クリデンシャルを有する。このマーチャント製品クリデンシャルは、ネットワーク放送局によってのみ作成され得る。

テレビ公告、インフォマーシャルまたはホームショッピングチャンネルは、製品を表示するので、ケーブルテレビネットワークも、簡単な説明、価格、およびマーチャント製品クリデンシャルを説明する同時デジタル情報を放送する。このデジタル情報は C P T によって処理されて一時的に格納され、購入の決断がなされれば、個人によって直ちにアクセスできる。

現在表示されている物を購入するためには、個人は、C P Tに命令を与えて、現在視聴している製品に関する文字情報をスクリーン上に表示させる専用テレビリモコンのオンスクリーン表示機能を選択する。

個人は、まず、オンスクリーンディスプレイを介して購入するアイテムの希望数の入力をプロンプトにより促される。次に、その個人のバイオメトリックP I C、およびその個人のアカウントインデックスコードの入力をプロンプトにより促される。その個人が最終購入額が適切であると検証するとすぐに、バイオメトリックP I Cとともに、製品、価格、マーチャントコード、マーチャント製品クリデンシャル、およびチャネル番号を使用して、遠隔トランザクション承認リクエストメッセージが作成される。このリクエストは、ケーブルテレビジョン広帯域双方向通信チャネルを用いて、承認のためにマーチャントに送信される。

このような手法で製品を購入することを望むマーチャントは、各自、広帯域ケーブルテレビジョンネットワークを使用して注文情報を受信することが可能である必要がある。

承認リクエストの受信に伴って、マーチャントはそれを、安全なインターネット接続またはX. 25接続を使用してD P Cに入力する。

D P Cがトランザクションを承認すると、承認コードに加えて個人の宛先、および暗号化された秘密コードを含む承認レスポンスを作成する。マーチャントは、承認を受信するとすぐに、承認、および郵送住所をコピーし、次に承認を転送してC P Tに戻し、次にC P Tは、個人に秘密コードを表示し、トランザクションを終了する。

このアーキテクチャは、犯罪者がケーブルT V広帯域から受信したメッセージを再生することを許可しないが、彼らがそれらを部分的に読むことは可能である。これが望ましくない場合には、(業界で知られている)C A T VセットトップボックスとC A T Vローカルオフィスとの間で、オプションであるC A T Vセンター

の公開鍵、または他の「リンクレベル」暗号化を使用して、メッセージを暗号化し得る。

マーチャントとD P Cとの接続を安全にするために、この接続は、公開鍵暗号化鍵交換システムを使用して予め交換された、毎日変更されるセッション鍵を使用する。

システム記述：データプロセッシングセンタ

データプロセッシングセンタ（D P C）は、その責任下における主な仕事として、金融取引承認（financial transaction authorizations）と個人の登録とを扱う。さらに、D P Cは、安全なファクス（secure faxes）、電子ドキュメントおよび電子署名のための、記憶と取出しとを提供する。

それぞれのD P Cサイトは、D P C概略図（番号**）に示されるように、L A N（当該分野において公知）によって、ともに接続された多くのコンピュータおよびデータベースからなっている。複数の同一のD P Cサイトは、どの一つのD P Cサイトで、災害または深刻なハードウェアの故障に直面しても、信頼あるサービスを確実にする。さらに、それぞれのD P Cサイトは、電源バックアップおよびD P Cの重要なハードウェアおよびデータベースシステムの全てにおいて、複数の重複を有する。

D P Cコンポーネントは、3つのカテゴリに分かれる。ハードウェア、ソフトウェアおよびデータベースである。下記は、カテゴリによる、それぞれのコンポーネントの簡潔な記述である。より詳細な記述は、次のセクションに現れる。

FW：

ファイアウォールマシン（Firewall Machine）：D P Cサイトのエントリ点。

GM：

ゲートウェイマシン（Gateway Machine）：システムコーディネータおよびメッセージプロセッサ。

D P C L A N

D P Cローカルエリアネットワーク（D C P Local Area Network）：D P Cサイト

を接続する。

データベース

I B D

個人のバイオメトリックデータベース (Individual Biometric Database) : 個人のバイオメトリックおよびP I Cコードから個人を識別する。

P F D

以前の詐欺のデータベース (Prior Fraud Database) : システムに対して詐欺行為を行った個人をリストし、バイオメトリックがそれらの個人のいずれかに一致すれば、チェックすることができる。

V A D

有効な装置のデータベース (Valid Apparatus Database) : B I Aメッセージの有効性を検査し復号化するのに要求される情報を記憶する。

A O D

装置のオーナーのデータベース (Apparatus Owner Database) : B I Aデバイスのオーナーに関する情報を記憶する。

I D

発行者データベース (Issuer Database) : システムに参加する発行銀行を識別する。

A I D

承認された個人データベース (Authorized Individual Database) : パーソナルまたは発行者B I Aデバイスを用いることが許された個人のリストを記憶する。

R M D

リモートマーチャントデータベース (Remote Merchant Database) : 電話およびケーブルテレビジョンマーチャントとともに取引を処理するために必要な情報を記憶する。

E D D

電子ドキュメントデータベース (Electronic Document Database) : 承認された個人による取出しのために、ファクスおよび電子メール等の、電子ドキュメン

トを記憶する。

E S D

電子署名データベース (Electronic Signature Database) : 第3者による有効性証明のために、電子ドキュメント署名を記憶する。

ソフトウェア

M P M

メッセージプロセッシングモジュール (Message Processing Module) : 他のソフトウェアモジュールとメッセージのタスクを実行するために要求されるデータベースとに整合することで、それぞれのメッセージのプロセッシングを取り扱う。

S N M

シーケンス番号モジュール (Sequence Number Module) : D U K P T シーケンス番号プロセッシングを取り扱う。

M A C M

メッセージ承認コードモジュール (Message Authentication Code Module) : M A C の有効性の証明および生成を取り扱う。

M D M

メッセージ復号化モジュール (Message Decrypt Module) : B I A 要求およびレスポンスの暗号化および復号化を取り扱う。

P G L

P I C グループリスト (P I C Group List) : P I C と、P I C グループのリストに依存するデータベースエレメントの構成とによって、P I C グループのルックアップを取り扱う。

I M L

I B D マシンリスト (I B D Machine List) : 所定の P I C グループのために I B D レコードを保持することを専門とした、メインおよびバックアップデータベースマシンのルックアップを取り扱う。

術語

データベースのスキーマ (schema) を定義する際に、次の術語がフィールドタイプを記述するために用いられる。

int <X>	<X> バイトの記憶を用いる整数タイプ
char <X>	<X> バイトの文字列
テキスト	可変長文字列
<タイプ> [X]	特定のタイプの長さ <X> の配列
時間	時間および日付を記憶するために用いられるタイプ
バイオメトリック	バイオメトリックを記憶するために用いられるバイナリデータタイプ
ファクス	ファクス画像を記憶するために用いられるバイナリデータタイプ

データベースの記憶要件を記述する際に、語「expected」は、完全にロードされたシステムの予想される状況を意味する。

プロトコルの説明

ターミナルは、DPCサイトにリクエストパケットを送信することによってそのタスクを成し遂げる。DPCサイトは、そのリクエストの成功または失敗に関するステータスを含む応答パケットを送り返す。

通信は、X.25接続、TCP/IP接続、またはモデムバンクへの電話呼出などの論理的または物理的な接続によるメッセージ配送メカニズムを介して行われる。各セッションでは、DPCがその応答をターミナルに送り返すまでターミナルへの接続が保持される。

リクエストパケットは、BIAメッセージ部およびターミナルメッセージ部を含む。

BIAメッセージ部

プロトコルバージョンNo.

メッセージタイプ

4 - バイトBIA識別

4 - バイトシーケンスNo.

〈メッセージ特定データ〉

メッセージ認証コード (MAC)

ターミナルメッセージ部

〈ターミナル特定データ〉

BIAメッセージ部は、BIAデバイスによって作成される。BIAメッセージ部は、1つまたは2つのバイオメトリック、PIC、承認量、およびターミナルによって設定される一般的なレジスタのコンテンツを含む。

注：BIAメッセージ部のMACは、BIA部にのみ適用され、ターミナル部には適用されない。

ターミナルは、リクエストメッセージに関する他のデータをターミナルメッセージ部に配置し得る。BIAは、メッセージ鍵を提供し、ターミナルがターミナル部データを確保できるようにする。BIAは、必要に応じて、メッセージ鍵をパケットの暗号化バイオメトリック-PICブロックに自動的に含む。しかし、ターミナルは、メッセージ鍵暗号化自体を実施する。

レスポンスパケットは、標準ヘッダと、MACを有する部およびMACを有さない部の2つのオプションフリー形態のメッセージ部とを含む。

標準ヘッダ

プロトコルバージョンNo.

メッセージタイプ

〈メッセージ特定データ〉

MAC

MACを有さないオプションフリー形態のメッセージ部

〈他のメッセージ特定データ〉

MACを有するメッセージ部は、BIAに送信され、この部分の応答に不正変更が加えられず、個人の秘密コードが表示されていないことの有効性を証明し得る。MACを有さないメッセージ部は、BIAのターミナル接続の帯域が限定され得るため、

MAC有効性の証明のためにBIAに送信されないファックス画像などの大量のデータを送信するために用いられる。

処理パケット

多数のDPCサイトを有する本発明の実施態様において、ターミナルは、そのリクエストをDPCサイトの1つ（通常最も近いサイト）にのみ送信する必要がある。なぜなら、そのサイトは、必要に応じて、配布されたトランザクションを実行することによってその他のサイトの更新を自動的に取り扱うからである。

DPCのファイアウォールマシン（Firewall Machines）の1つがパケットを受信すると、そのマシンはそのパケットをGMマシンの1つにフォワードして実際の処理を行う。各GMは、リクエストを処理するために必要なDPC構成要素間の協調を取り扱い、応答を送信者に送り返すメッセージ処理モジュールを有する。

パケットの有効性の証明および復号化

DPCが受信するBIAによって作成されないパケットを除くすべてのパケットは、BIAハードウェア識別コード（パケットのBIA識別）、シーケンスNo.、およびメッセージ認証コード（MAC）を含む。GMは、MACモジュールにパケットMACの有効性を証明するように要求し、次に、シーケンスNo.モジュールを用いてシーケンスNo.をチェックする。この2つが確認されると、GMは、パケットをメッセージ復号化モジュールに送りパケットを復号化する。いずれか1つが確認されない場合には、GMは、警告をログし、パケットの処理を停止し、エラーメッセージをBIAデバイスに戻す。

現在、BIAによって作成されないメッセージタイプは、安全ファックスデータリクエストおよび電子文書データリクエストのみである。

応答パケット

DPCが受信する各パケットは、パケットの暗号化バイオメトリックPICブロックに格納されるオプションル応答鍵を含んでいてもよい。DPCは、応答鍵を含むリクエストに応答する前に、応答パケットを応答鍵で暗号化する。さらに、DPC

は、メッセージ認証コードを生成し、それをパケットに追加する。

レスポンスパケットを暗号化しない唯一の例外としてエラーメッセージが挙げられる。エラーは暗号化されず、機密情報を含まない。しかし、大抵のレスポンスパケットは、リクエストが成功したか否かを示すことができるステータスまた

は応答コードを含む。例えば、DPCがクレジット認証を拒否するとき、DPCはエラー packets を戻さずに、「失敗 (failed)」と設定された応答コードを有する通常のトランザクションレスポンス packets を戻す。

DPC プロシージャ

DPCは、リクエストを処理する間に通常用いられる2つのプロシージャ、即ち、個人識別プロシージャおよび緊急応答プロシージャを有する。

個人識別プロシージャ

DPCが個人を識別することを要求するリクエストの場合、DPCは、以下のプロシージャを実行する： DPCは、PICコードを用いて、IBDマシンリストをサーチしてこの与えられたPICコードに対する識別を取り扱う主要IBDマシンおよびバックアップIBDマシンを求める。次に、DPCは、主要マシンまたはバックアップマシンのいずれかのロードの少ない方に識別リクエストを送信する。IBDマシンは、個人に関するIBDレコードまたは「個人不明 (individual no found)」エラーを用いて応答する。

IBDマシンは、与えられたPICに対するすべてのIBDレコードを取り出す。所有者バイオメトリックハードウェアデバイスを用いて、IBDマシンは、各レコードの第一のバイオメトリックと、個人のバイオメトリックとを比較し、これら2つのバイオメトリックの類似性を示す比較スコアに到達する。いずれのバイオメトリックも十分な類似性を有する比較スコアを有さない場合、第二のバイオメトリックを用いて比較が繰り返される。第2のバイオメトリックのいずれも十分な類似性を有する比較スコアを有さない場合、IBDマシンは、「個人不明」エラーを戻す。あるいは、IBDマシンは、秘密コード、アカウントNo.、タイトル、等のフィールドが得られる個人のIBDレコード全体を戻す。

緊急応答プロシージャ

アカウントインデックスを含むリクエストに関しては、DPCは、個人がその緊急アカウントインデックスを選択する場合を取り扱う。リクエストがDPCカスタマサポートスタッフに即座に通知するGM処理では、警告がログされ、レスポンス packets が応答コードを有する場合、そのレスポンス packets は「緊急」とし

て設定される。「緊急」応答コードに注意し、ATMターミナルセクションに記載されるような疑似スクリーンメカニズムなどのさらなる援助を提供するのは、リクエストを入力したBIAデバイスのオーナーの責任である。DPCはまた、緊急アカウントインデックスがアクセスされる度に、個人のIBDレコードの緊急使用カウントを増加させる。

プロトコルリクエスト

以下のセクションでは、各プロトコルのリクエスト／応答およびそのプロトコルを実施するためにDPCが行うアクションについて記載する。

プロトコルパケットのリストは、

個人識別

トランザクション承認

登録

アカウントアクセス

発行者バッチ

安全ファックス入力

安全ファックスデータ

安全ファックス追跡

安全ファックス取り出し

安全ファックス拒否

安全ファックスアーカイブ

安全ファックス契約受理

安全ファックス契約拒否

安全ファックス機構変更

電子文書入力

電子文書データ

電子文書追跡

電子文書取り出し

電子文書拒否

電子文書アーカイブ

電子文書アーカイブ取り出し

電子署名

電子署名検証

ネットワーククリデンシャル

個人識別

個人識別リクエスト

BIA部：

4-バイトBIA識別

4-バイトシーケンスNo.

暗号化（DUKPT鍵）バイオメトリック-PICブロック

300-バイト承認バイオメトリック

4-12ディジットPIC

56-ビット応答鍵

MAC

ターミナル部：（使用されない）

個人識別応答

暗号化（応答鍵）：

秘密コードテキスト

個人名

バイオメトリック識別コード

MAC

個人識別リクエストは、バイオメトリック-PICブロックを有し、DPCはこのブロックを個人識別プロシーダを用いて使用し、個人を識別する。個人が識別されると、DPCは、個人の名前、バイオメトリック識別、および秘密コードを用いて応答する。あるいは、DPCは、「個人不明」エラーを用いて応答する。

トランザクション承認

トランザクション承認リクエスト

BIA部：

4-バイトBIA識別

4-バイトシーケンスNo.

暗号化（DUKPT鍵）バイオメトリック-PICブロック：

300-バイト承認バイオメトリック

4-12ディジットPIC

56-ビット応答鍵

[オプション56-ビットメッセージ鍵]

アカウントインデックス

価格

マーチャント識別

[オプションフリーフォーマット製品情報]

[オプションマーチャントコード（電話#、チャンネル#+時間、店主名）

]

[オプション送信アドレスリクエスト]

MAC

ターミナル部：（使用されない）

トランザクション承認応答

暗号化（応答鍵）：

秘密コードテキスト

承認応答

承認詳細（承認コード、トランザクション識別、等）

[オプション個人アドレス情報]

応答コード（失敗、ok、緊急）

MAC

2つの基本的なトランザクション承認サブタイプ、即ち、リテイル承認および遠隔承認がある。

リテイル承認に関しては、DPCは、リクエストのバイオメトリック-PICブロッ

クによって購入者個人を識別する。個人を識別することができない場合には、DPCは、「個人不明」エラーを用いて応答する。

次に、DPCは、外部承認リクエスト（BIAデバイスのオーナーの資産アカウントに対する貸方の記入および個人資産アカウントに対する借方の記入）を、関係する資産アカウントのタイプ（ビザまたはアメリカンエクスプレスなど）に応じて、いくつかの現存する経済的承認サービスの1つに送信する。外部経済的承認サービスがトランザクションを認める場合、DPCは、外部承認コードおよび「ok」応答コードをBIAデバイスに戻す。あるいは、DPCは、承認が拒否された理由を戻し、応答コードを「失敗」に設定する。いずれにせよ、DPCは、応答中に個人の秘密コードを含む。

DPCが、リクエストのアカウントインデックスを用いて個人の資産アカウントを調べるとき、選択されたアカウントは、「緊急」のアカウントであり得る。このようなことが発生する場合、DPCは、緊急応答プロシージャに従う。しかし、それでも外部承認は発生する。

遠隔承認は、電話、メールオーダー、またはケーブルテレビマーチャントによって発生する。DPCは、以下を除いて、リテイル承認と同様に遠隔承認を取り扱う。

i) 遠隔承認は、遠隔マーチャントコードを有し、DPCはこのコードを遠隔マーチャントデータベースと照合してチェックし、パケットのマーチャント識別がデータベースに格納されたものと一致するかどうかの有効性を検証する。さらに、貸方に記入された資産アカウントは、遠隔マーチャントのアカウントであって、

BIAデバイスのオーナーのアカウントではない。

ii) さらに、遠隔承認を発生させるBIAデバイスは、個人のBIAデバイスである場合が多い。DPCは、BIAデバイスの使用を許可された個人の承認された個人データベースリストと照合して識別された個人のバイオメトリック識別をチェックする。個人がデバイスの使用を承認されていない場合には、DPCは、承認リクエストを拒否する。

iii) 最後に、承認パケットは、「送信アドレス」インジケータを含み得る。こ

のインジケータは、DPCに個人のアドレスを応答パケットに含むように通知し、通常、メールオーダー購入に対してのみ使用される。

登録

登録リクエスト

B I A 部：

4-バイト B I A 識別

4-バイト シーケンス番号

暗号化された (D U K P T) バイオメトリック- P I C ブロック：

1000-バイト 第1のバイオメトリック

1000-バイト 第2のバイオメトリック

4-12ディジット P I C

56-ビット レスポンス鍵

56-ビット メッセージ鍵

M A C

ターミナル部：

暗号化された (メッセージ鍵)：

名前

住所

郵便番号

秘密コード

資産アカウントリスト (アカウントインデックスコード、アカウント番号)

緊急アカウント (アカウントインデックスコード、アカウント番号)

タイトルリスト (タイトルインデックスコード、タイトル名)

登録レスポンス

ステータスコード

暗号化された (レスポンス鍵)

秘密コードテキスト

P I C

バイオメトリック識別コード

D P C 選出 P I C リスト（元々選択された P I C が拒否された場合）

ステータスコード（o k、拒否）

M A C

個人は、バイオメトリック登録ターミナル（B R T）を通じて D P C に登録を行う。B R T は、個人の名前、住所、金融資産アカウントのリスト、秘密コードおよび緊急アカウントといった付属的データとともに、第 1 のおよび第 2 のバイオメトリック、および個人識別コードを含む登録パッケージを D P C に送信する。任意に、個人は電子メールアドレス、ならびにタイトルおよびタイトルインデックスコードを有するタイトルリスト、さらに社会保障番号（すなわち「S S N」）を含ませ得る。個人は、自分の P I C コードを選んでもよいし、システムに選ばせてもよい。改変ステップにおいて、以前に入力されたいかなるデータも改変、または削除できる。

容易に実施できるように、どの所与の時点においても、登録サイトとして機能するのはある一つの D P C サイトだけである。非登録 D P C サイトが受け取った登録リクエストパッケージは、現在の登録サイトにフォワードされる。登録 D P C サイトは、登録チェック全体、I B D マシンへの I B D 記録の割り当て、および他の全ての D P C サイトを更新するために必要な、ディストリビューティドトランザクション(distributed transaction)を行う。

ランザクション(distributed transaction)を行う。

登録 D P C サイトは、他の D P C サイトを更新するためにディストリビューティドトランザクションを実行する前に、登録リクエストに対して、P I C コードを指定していないものについて選出し、I B D 記録を（P I C グループリストにおいて指定される）メインおよびバックアップ I B D マシンに格納し、P I C および登録パッケージのバイオメトリック適合性をチェックする。

D P C は、個人識別コードおよびバイオメトリックサンプル複製チェックステップを実行し、登録ステップ中に集められたバイオメトリックスおよび個人識別コードを、同一の個人識別コードに現在関連づけられている、以前に登録された

全てのバイオメトリックスに対してチェックする。D P Cは、次のような理由で登録を拒否し得る：P I Cコードが一般的すぎる、あるいは、バイオメトリックスが、選ばれたP I C下に格納された他のバイオメトリックスと類似しすぎている。許容可能なP I Cを選ぶ際に個人を助けるべく、D P Cは、それについては登録されることが確実に保証されるP I Cコードの短いリストを生成し、これを一定期間保存する。B R Tは次に、個人にプロンプトを与えて、新しいP I Cの入力を促すか、この新しいP I Cは、上記適合P I Cリストから選出されてもよい。

アカウント（口座）アクセス

アカウントアクセスリクエスト

B I A部：

4-バイト B I A識別

4-バイト シーケンス番号

暗号化された（D U K P T鍵）バイオメトリック-P I Cブロック：

300-バイト 承認バイオメトリック

4-12ディジット P I C

56-ビット レスポンス鍵

[任意の56-ビット メッセージ鍵]

アカウントインデックス

M A C

ターミナル部：（不使用）

アカウントアクセスレスポンス

暗号化された（レスポンス鍵）：

秘密コードテキスト

[任意のP I C]

資産アカウント番号

返答コード（失敗、o k、緊急）

M A C

アカウントアクセスリクエストにより、B I Aを装備した自動預金支払機が、個人がA T Mに対して身分証明を行う、より安全で便利な方法を提供することが可能になる。

G Mは、パケットのバイオメトリックP I Cによって個人を識別し、指定されたアカウントインデックスを用いて、どの資産アカウント番号を取り出すのかを選ぶ。

リクエストのアカウントインデックスを用いて、G Mが個人の資産アカウントをルックアップするとき、選ばれたアカウントは、「緊急」アカウントであり得る。このことが起こった場合、G Mは緊急レスポンスプロシージャに従う。

発行者バッチ

発行者バッチリクエスト

B I A部：

4-バイト B I A識別

4-バイト シーケンス番号

暗号化された（D U K P T鍵）バイオメトリックP I Cブロック：

300-バイト 承認バイオメトリック

4-12ディジット P I C

56-ビット レスポンス鍵

56-ビット メッセージ鍵

発行者コード

M A C

ターミナル部：

暗号化された（メッセージ鍵）

a d d 〈バイオメトリック I d〉 〈アカウントインデックス〉 〈資産アカウント〉 [〈緊急フラグ〉]

r e m o v e 〈バイオメトリック I d〉 〈アカウントインデックス〉 〈資産アカウント〉

発行者バッチレスポンス

暗号化された（レスポンス鍵）：

秘密コードテキスト

返答コード（失敗、o k、緊急）

M A C

暗号化された（メッセージ鍵）失敗リスト：

失敗した〈コマンド〉〈コード〉

．．．

発行者バッチリクエストにより、発行銀行またはその他の機関が個人バイOMETリックデータベースのルーチン維持を行うことが可能になる。D P Cはまた、D P Cが非発行者B I Aデバイスから発行者バッチリクエストを受け取った場合、セキュリティ違反警告(security violation warning)を記録し、またリクエストの処理を拒否する。

D P Cは、個人識別プロシージャに従ってバッチリクエストを入力している個人を識別する。D P Cは次に、個人が承認された個人データベースに登録され、送信発行者ターミナル内にあるB I Aデバイスを使用できる状態にあることをチ

ェックする。

D P Cはまた、リクエスト内の発行者コードを用いて発行者データベース内の装置所有者識別をルックアップし、それを有効装置データベース内に格納される装置所有者識別に対して比較して発行者コードが偽造されていないことを確認する。

D P Cは次にメッセージ鍵により暗号化されたバッチリスト内のコマンドの追加および削除を実行する。バッチリストは、復帰改行分割コマンドリスト(new line separated list of commands)である。有効コマンドは以下のとおりである。

a d d（追加）〈バイOMETリック I d〉〈アカウントインデックス〉〈資産アカウント〉 [〈緊急フラグ〉]

追加コマンドは、指定されたアカウントインデックスのアカウントリストに資産アカウントを追加する。任意の緊急フラグは、特定のアカウントインデックスが個人の緊急アカウントとして取り扱われたかどうかを示す。現在アカウントリ

ストに格納されている資産アカウントが発行者のものではない場合、コマンドは失敗する。この特徴により、ある銀行が、個人の認知あるいは承認なしで他の銀行の顧客の資産アカウントを追加または除去することを防ぐ。

remove (除去) 〈バイオメトリック I d〉 〈アカウントインデックス〉 〈資産アカウント〉

除去コマンドは、アカウントリスト内の指定されたアカウントインデックスに格納された個人の資産アカウントを消去する。現在アカウントリストに格納されている資産アカウントが、発行者が除去しようとしているアカウントに一致しない場合、コマンドは失敗する。

正しく実行することに失敗したバッチ内のコマンド各々について、GMがセキュリティ違反警告を記録し、失敗したレスポンスのリストにエントリを添付(appends)する。失敗したエントリは、コマンドのテキストおよびエラーコードを含む。

安全ファックス入力

安全ファックス入力リクエスト

B I A 部：

4-バイト B I A 識別

4-バイト シーケンス番号

暗号化された (D U K P T 鍵) バイオメトリック- P I C ブロック：

300-バイト 承認バイオメトリック

4-12ディジット P I C

56-ビット レスポンス鍵

56-ビット メッセージ鍵

セキュリティモード (保証無(unsecured)、送り手保証(sender-secured)、保証(secured)、保証秘匿(secured-confidential))

送り手タイトルインデックスコード

送り手ファックス番号

送り手ファックス内線

受け手リスト

[任意のアーカイブファックスインジケータ]

[任意の契約／同意インジケータ]

ターミナル部：（不使用）

安全ファックス入力レスポンス

暗号化された（レスポンス鍵）

秘密コードテキスト

ファックストラッキング番号

MAC

D P Cが安全ファックス入力リクエストを受け取るとき、D P Cは、個人識別プロシージャに従って、リクエストのバイオメトリックP I Cから個人を識別

する。タイトルインデックスで記述された個人のタイトルとともに、この識別は受取人に提示され、そのことによってファックスの送り手は常時確実に識別される。

D P Cがトラッキングの目的でトラッキング番号を生成し、そのトラッキング番号、送り手のバイオメトリック識別、セキュリティモード、およびメッセージ鍵を新しく作成されたE E D文書記録内に格納する。受け手リスト内の受け手各々に対して、D P Cは、受け手記録も作成する。D P Cは次に、送信中のファックスマシーンがこのメッセージ鍵で暗号化されたファックスデータを送信するのを待つ。

リクエストが「アーカイブファックス」または「契約／同意」インジケータを含んでいる場合、E D Dは、文書および受け手記録のコピーをアーカイブデータベースに入れる。これらの記録への以降の更新は全て保存版(archived version)にされる。

ファックスデータは別のステップで送信され、これにより送り手がバイオメトリックおよびP I Cの入力を間違えた場合、ファックスマシーンに文書をフィードする時間を浪費する前にシステムが送り手に通知する。

安全ファックスデータ

安全ファックスデータリクエスト

B I A 部：（不使用）

ターミナル部：

ファックストラッキング番号

暗号化された（メッセージ鍵）：

ファクスイメージデータ

安全ファックスデータレスポンス

ステータス（未完、o k）

安全ファックスデータリクエストは、安全ファックスマシンに、ファックスイメージをD P Cに送って前に指定した受け手への送信を行わせる。このリクエストは、安全にイメージを送信するために、バイオメトリック識別およびそれに代わるシークレットメッセージ鍵に依存するものを含んでいない。

ファックスイメージデータは、安全ファックス入力リクエストにより登録されるメッセージ鍵によって暗号化される。D P Cがファックス全体を受け取ってしまえば、D P Cは、各受け手のファックス番号へ安全ファックス着信通知(Secure Fax Arrival Notice)メッセージを送る。D P Cは、ファックストラッキング番号を有する全ての受け手記録についてE D Dを照会することによって、受け手リストを取り出す。受け手記録はデスティネーションファックス番号および任意の拡張を有している。着信通知を送信後、D P Cは、各受け手記録の送信ステータスフィールドを「通知済み」へと更新する。注：デスティネーションファックス番号がビジーの場合、D P Cが送信ステータスフィールドに「ビジー」と記し、成功するまで通知を定期的（例えば10分毎）に送信を再試行し、成功した時にはステータスフィールドを「通知済み」に更新する。

着信通知は以下のようなものである。

安全ファックス着信通知（ファックスメッセージ）

送り手の名前、会社名(company)、タイトル、およびファックス番号

ファックストラッキング番号

ファックスのダウンロード方法についての指示

D P Cは、全ての受け手がファックスを取り出したり拒否した後にファックスを介して、送り手にステータス通知を送るだけである。送り手は、安全ファックストラッキングリクエスト（下記参照）を用いてD P Cを照会し、受け手全員の現在のステータスを得る。

安全ファックスステータス通知（ファックスメッセージ）

安全な送り手の名前、会社名、タイトル、およびファックス番号

ファックストラッキング番号

以下のものを示す受け手リスト：

名前、会社名、タイトル、およびファックス番号

送信データおよびステータス

契約／同意ステータス

D P Cは、E D D組織テーブル内の個人の会社名およびタイトル情報のそれぞれを検索する。システムに登録されておらず、従って安全ファックスを受け取ることができない個人、あるいは非受け手安全モードの場合、D P Cは、安全ファックス着信通知を送らない。その代わりに、D P Cは、ファックスを直接送る。ファックスラインがビジーの場合、D P Cはファックスの送信に成功するまで10分毎に再試行を行う。

ファックストラッキング

安全ファックストラッキングリクエスト

B I A部：

4-バイト B I A識別

4-バイト シーケンス番号

暗号化された（D U K P T鍵）バイオメトリック-P I Cブロック：

300-バイト 承認バイオメトリック

4-12ディジット P I C

56-ビット レスポンス鍵

56-ビット メッセージ鍵

ファックストラッキング番号

MAC

ターミナル部：（不使用）

安全ファックストラッキングレスポンス

暗号化された（レスポンス鍵）：

秘密コードテキスト

トラッキングレスポンスファックスイメージのメッセージダイジェスト

ステータスコード（ok、失敗）

MAC

受け手ステータスリストのファックスイメージ

DPCは、そのファックスについての全てのEDD受け手記録を引き出すことにより、および記録を表示するためのファックスメッセージを生成することにより、安全ファックストラッキングリクエストを処理する。トラッキングリクエストを行っている個人がファックス文書の送り手ではない場合、DPCはステータスコードを失敗にセットし、レスポンスに空ファックスを入れる。

トラッキングレスポンスファックスは、受け手各々に対する送信ステータスを説明する情報を含んでいる。このファックスは、ラインビジー、ファックス着信通知送信済み、ファックス送信済み、ファックス拒否、契約受諾、などのステータス情報を含んでいる。

トラッキング通知は以下のとおりである。

安全ファックストラッキング通知（ファックスメッセージ）

送り手の名前、会社名、タイトル、およびファックス番号

ファックストラッキング番号

以下のものを示す受け手リスト：

名前、会社名、タイトル、およびファックス番号

送信データおよびステータス

契約ステータス

安全ファックス取り出し

安全ファックス取り出しリクエスト

B I A 部：

4-バイト B I A 識別

4-バイト シーケンス番号

暗号化された（D U K P T 鍵）バイオメトリック- P I C ブロック：

300-バイト 承認バイオメトリック

4-12ディジット P I C

56-ビット レスポンス鍵

ファックストラッキング番号

M A C

ターミナル部：（不使用）

安全ファックス取り出しレスポンス

暗号化された（レスポンス鍵）：

秘密コード

56-ビットメッセージ鍵

ステータス（未完、o k、受け手無効）

ファックスイメージのメッセージダイジェスト

M A C

暗号化された（メッセージ鍵）：

ファックスイメージ

D P C はバイオメトリック- P I C を用いて、個人識別プロシージャに従って取り出しリクエストを行っている個人を識別する。その個人および指定されたファックスに関して E D D 受け手記録が存在しない場合、D P C は、「受け手無効」ステータスを返す。

D P C は暗号化されたファックスイメージを、正しいファックストラッキング番号、および要求者に返信されるバイオメトリック識別とともに E D D ドキュメント記録から取り出す。

ファックスイメージは、ファックスが契約／同意のものかどうかを、および送り手の名前、会社名、タイトル、ファックス番号、および拡張(extension)を表

示するカバーページを含んでいる。

最後の受け手がファックスの受取りあるいは拒否のどちらかを完了すると、D P Cは、そのファックスの送り手にファックスを介してステータス通知を送り（上記の安全ファックスデータ参照）、次に設定可能時間内にE D Dから文書および受け手記録を削除するように予定を立てる。この時間は、ファックスをアーカイブするかどうかを決定するのに十分な時間を受け手に与えるためのものである。

安全ファックス拒否

安全ファックス拒否リクエスト

B I A部：

4-バイト B I A識別

4-バイト シーケンス番号

暗号化された（D U K P T鍵）バイオメトリックP I Cブロック：

300-バイト 承認バイオメトリック

4-12ディジット P I C

56-ビット レスポンス鍵

ファックストラッキング番号

M A C

ターミナル部：（不使用）

安全ファックス拒否レスポンス

暗号化された（レスポンス鍵）：

秘密コード

ステータスコード（o k、受け手無効）

M A C

D P CはバイオメトリックP I Cを用いて、安全ファックス拒否リクエストを行っている個人を識別する。D P Cは、リクエストのファックストラッキング

番号および個人のバイオメトリック識別によって鍵がかけられたE D D受け手記録を検索する。この記録が見つからない場合、リクエストは「受け手無効」ステ

ータスとともに失敗する。

最後の受け手がファックスの受取りあるいは拒否のどちらかを完了すると、D P Cは、そのファックスの送り手にファックスを介してステータス通知を送り（上記の安全ファックスデータ参照）、次に設定可能時間内にE D Dからファックスおよびトラッキング記録を削除するように予定を立てる。この時間は、ファックスをアーカイブするかどうかを決定するのに十分な時間を受け手に与えるためのものである。

安全ファックスアーカイブ

安全ファックスアーカイブリクエスト

B I A部：

4-バイト B I A 識別

4-バイト シーケンス番号

暗号化された（D U K P T 鍵）バイオメトリック—P I C ブロック：

300-バイト 承認バイオメトリック

4-12ディジット P I C

56-ビット レスポンス鍵

ファックストラッキング番号

M A C

ターミナル部：（不使用）

安全ファックスアーカイブレスポンス

暗号化された（レスポンス鍵）：

秘密コード

ステータスコード（o k、個人無効）

M A C

D P Cはバイオメトリック—P I Cを用いて、安全ファックスアーカイブリクエストを行っている個人を識別する。D P Cは、リクエストのファックストラッキング番号および個人のバイオメトリック識別によって鍵がかけられたE D D受け手記録を検索する。この記録が見つからず、個人が送り手でも受け手の一人で

もない場合、リクエストは「個人無効」ステータスとともに失敗する。そうでなければDPCは、EDDアーカイブデータベースの中に文書および受け手記録をコピーする。これら記録への以降の変更は全て、保存版へコピーされる。

安全ファックス契約受諾

安全ファックス契約受諾リクエスト

BIA部：

4-バイト BIA識別

4-バイト シーケンス番号

暗号化された(DUKPT鍵)バイオメトリック-PICブロック：

300-バイト 承認バイオメトリック

4-12ディジット PIC

56-ビット レスポンス鍵

ファックストラッキング番号

MAC

ターミナル部：(不使用)

安全ファックス契約受諾レスポンス

暗号化された(レスポンス鍵)：

秘密コード

ステータスコード(ok、受け手無効)

MAC

DPCはバイオメトリック-PICを用いて、契約受諾リクエストを行っている個人を識別する。DPCは、リクエストのファックストラッキング番号および

個人のバイオメトリック識別によって鍵がかけられたEDD受け手記録を検索する。この記録が見つからない場合、リクエストは「受け手無効」ステータスとともに失敗する。そうでなければDPCは、受け手記録の契約ステータスフィールドを「受諾」に更新し、またファックスの送り手に対してステータス通知を生成する(上記ファックスデータ参照)。

安全ファックス契約拒否

安全ファックス契約拒否リクエスト

B I A 部：

4-バイト B I A 識別

4-バイト シーケンス番号

暗号化された（D U K P T 鍵）バイオメトリック-P I C ブロック：

300-バイト 承認バイオメトリック

4-12ディジット P I C

56-ビット レスポンス鍵

ファックストラッキング番号

M A C

ターミナル部：（不使用）

安全ファックス契約拒否レスポンス

暗号化された（レスポンス鍵）：

秘密コード

ステータスコード（o k、個人無効）

M A C

D P C はバイオメトリック-P I C を用いて、契約拒否リクエストを行っている個人を識別する。D P C は、リクエストのファックストラッキング番号および個人のバイオメトリック識別によって鍵がかけられた E D D 受け手記録を検索する。この記録が見つからない場合、リクエストは「受け手無効」ステータスと

もに失敗する。そうでなければ D P C は、受け手記録の契約ステータスフィールドを「拒否」に更新し、またファックスの送り手に対してステータス通知を生成する（上記ファックスデータ参照）。

安全ファックス組織変更

安全ファックス組織変更（安全ファックスメッセージ）

送り手の名前、会社名、タイトル、およびファックス番号

組織変更のリスト

組織変更は、安全ファックスメッセージを介して D P C に入力される。顧客サ

ポートエンジニアが、その特定の会社に個人を登録することをそのリクエストを入力している個人が許可されているかを確認しながら、ファックスメッセージにおいてリクエストされた変更を入力する。このファックスは安全ファックスなので、送り手の同一性は送り手のタイトル同様、確証済みである。

電子文書入力

電子文書入力リクエスト

B I A 部：

4-バイト B I A 識別

4-バイト シーケンス番号

暗号化された（D U K P T 鍵）バイオメトリック- P I C ブロック：

300-バイト 承認バイオメトリック

4-12ディジット P I C

56-ビット レスポンス鍵

56-ビット メッセージ鍵

受け手リスト

M A C

ターミナル部：（不使用）

電子文書入力レスポンス

暗号化された（レスポンス鍵）：

秘密コードテキスト

トラッキング番号

ステータスコード（o k、受け手無効）

M A C

D P C は、電子文書入力リクエストを受け取ると、個人識別プロシージャに従って個人を識別する。

D P C は次に E D D 文書記録を作成し、その E D D 文書記録に固有トラッキング番号を割り当てる。D P C は、記録の送り手識別コードを初期化して、識別した個人のバイオメトリック識別コードとし、またメッセージ鍵を初期化して、そ

のリクエストのメッセージ鍵とする。

次にDPCは、受け手各々について識別バイオメトリックデータベースをサーチし、各々一人についてEDD受け手記録を作成する。各記録を、トラッキング番号、受け手のバイオメトリック識別コード、および送信ステータス「未完」で初期化する。受け手が一人として見つからない場合、DPCは、「受け手無効」ステータスを返答する。

電子文書データ

電子文書データリクエスト

BIA部：（不使用）

ターミナル部：

トラッキング番号

コマンド（アボートあるいはデータ）

[任意のメッセージオフセット]

完了指標(indication)

暗号化された（メッセージ鍵）：

メッセージ本文

電子文書データレスポンス

ステータス（未完、ok）

電子文書データリクエストにより個人が文書テキスト（一部またはそれ以上の部分）をEDDに送って、受け手への送信を行うことが可能になる。このリクエストはバイオメトリック識別を全く用いず、代わりに、文書テキストを安全に送信するためのシークレットメッセージ鍵を用いている。

リクエストテキストは、EDD文書記録に格納されるメッセージ鍵によって暗号化されたものと仮定され、この記録に既に格納されている文書テキストに添付される。

EDDは、「文書完全性」インジケータを伴うパケットを受け取ったとき、送り手が文書の送信を完了したことを知る。次にEDDは、インターネット電子メールを介してその文書の受け手全員に着信通知を送り、受け手に待期文書がある

ことを知らせる。

着信通知は以下のとおりである。

電子文書着信通知（インターネットEメールメッセージ）

送り手の名前、会社名、タイトル、およびeメールアドレス
トラッキング番号

電子文書の受信に関する指示

EDDはまた、EDD受け手記録のステータスを「通知済」に更新する。全ての受け手とその電子文書の取出しあるいは拒否のいずれかを完了すると、DPC0は、インターネット電子メールを介して、文書編成者(document originator)にステータス通知を送る。

ステータス通知は以下の通りである。

電子文書ステータス通知（インターネットEメールメッセージ）

送り手の名前、会社名、タイトル、およびeメールアドレス
トラッキング番号

各人の名前、会社名、タイトル、eメールアドレスを示す受け手のリスト
送信データおよびステータス

DPCは、EDD組織テーブル内の個人の会社名およびタイトル情報の各々を検索する。

電子文書取り出し

電子文書取り出しリクエスト

BIA部：

4バイトBIA識別

4バイトシーケンス番号

暗号化された（DUKPT鍵）バイOMETリックPICブロック：

300バイト承認バイOMETリック

4-12ディジットPIC

56ビットレスポンス鍵

トラッキング番号

MAC

ターミナル部：（不使用）

電子文書取り出しレスポンス

暗号化（レスポンス鍵）：

秘密コード

56ビットメッセージ鍵

ステータス（未完、OK、受け手無効）

MAC

暗号化（メッセージ鍵）：

文書テキスト

DPCは、個人識別手続きに従って、電子文書取り出しリクエストを行っている個人を識別するためにバイオメトリックPICを使用する。

続いてDPCは、トラッキング番号及び個人のバイオメトリック識別子によって鍵をかけられたEDD受け手記録を発見する。

記録が発見できなければ、リクエストは「受け手無効」ステータスをもって失敗となる。それ以外の場合には、DPCは文書のメッセージ鍵及び（メッセージ鍵によって暗号化されたままの）文書を要求人に送る。

そしてEDDは、EDD受け手記録ステータスを「取り出し済み」に更新する。すべての受け手が文書の取り出しあるいは拒否を行ったら、DPCは文書編成者（上記電子文書データ参照）にインターネット電子メールでステータス通知を送り、そして文書記録及び受け手記録（上記安全ファックス取り出し参照）の削除の予定をたてる。

電子文書拒否

電子文書拒否リクエスト

BIA部：

4バイトBIA識別

4バイトシーケンス番号

暗号化された（DUKPT鍵）バイオメトリックPICブロック：

300バイト承認バイオメトリック

4-12ディジットPIC

56ビットレスポンス鍵

メッセージトラッキング番号

MAC

ターミナル部：（不使用）

電子文書拒否レスポンス

暗号化（レスポンス鍵）：

秘密コード

ステータスコード（OK、受け手無効）

MAC

DPCは、個人識別手続きに従って電子文書拒否リクエストを行っている個人を識別するためにバイオメトリックPICを使用する。

続いてDPCは、トラッキング番号及び個人のバイオメトリック識別子によって鍵をかけられたEDD受け手記録を発見する。

記録が発見できなければ、リクエストは「受け手無効」ステータスをもって失敗する。

EDDは、EDD受け手記録ステータスを「拒否」に更新する。そしてDPCは電子文書取り出しにおいて述べたものと同じ通知及び削除手続きを続けて行う。

電子文書アーカイブ

電子文書アーカイブリクエスト

BIA部：

4バイトBIA識別

4バイトシーケンス番号

暗号化された（DUKPT鍵）バイオメトリックPICブロック：

300バイト承認バイオメトリック

4-12ディジットPIC

56ビットレスポンス鍵

トラッキング番号

MAC

ターミナル部：（不使用）

電子文書アーカイブレスポンス

暗号化（レスポンス鍵）：

秘密コード

ステータスコード（OK、個人無効）

MAC

DPICは、個人識別手続きに従って電子文書アーカイブリクエストを行っている個人を識別するためにバイオメトリックPICを使用する。

DPICは、リクエストのトラッキング番号及び個人のバイオメトリック識別子によって鍵をかけられたEDD受け手記録を発見する。

記録が発見できず、その個人が送り主あるいは受け手の一人でない場合、リクエストは「個人無効」ステータスをもって失敗する。それ以外の場合には、DPICは文書及び受け手記録をEDDアーカイブデータベースにコピーする。それ以降のこれらの記録に対する変更は、全て保存版にコピーされる。

電子文書アーカイブ取り出し

電子文書アーカイブ取り出しリクエスト

BIA部：

4バイトBIA識別

4バイトシーケンス番号

暗号化された（DUKPT鍵）バイオメトリックPICブロック：

300バイト承認バイオメトリック

4-12ディジットPIC

56ビットレスポンス鍵

任意のタイトルインデックスコード、送信ファックス番号、内線

トラッキング番号

M A C

ターミナル部：（不使用）

電子文書アーカイブ取り出しレスポンス

暗号化（レスポンス鍵）：

秘密コード

ステータスコード（O K、個人無効）

M A C

D P Cは、安全ファックスターミナルあるいは認可された（Certified）Eメールターミナルいずれからも、電子文書アーカイブ取り出しリクエストを受けうる。D P Cは、アーカイブ取り出しリクエストを出している個人を判定するために、個人識別手続きを使用する。個人は送り主あるいは受け手の一人でなければならない。それ以外の場合は、D P Cはステータスコードを「個人無効」とすることによって、リクエストを拒否する。しかし、アーカイブ文書が法人名を用いて送られたファックスであるならば、D P Cは、その法人の位階制度上、より高い役職名を有する更なる個人にもアーカイブ文書の取り出しを許可する。

E D Dはアーカイブデータベースを保持するが、データベースは、文書の元のトラッキング番号によってインデックスされ、C D-R O Mやアーカイブ文書の取り出しにかなりの時間を要するテープのようなオフライン記憶媒体に格納される。その結果、D P Cはアーカイブ文書をすぐに返送するのではなく、それに代えてD P Cが検索を開始したことを要求人に報告する。後日、D P Cが検索を終えた時、もとの文書のフォーマットに応じて、ファックスやEメールといった標準的な文書着信通知メカニズムによって、保存された文書が取り出せる状態にあることを要求人に通知する。D P CはE D Dアーカイブリクエスト記録を生成して、要求人についての情報を格納し、それによって、検索が終了した際、D P Cはその文書を誰に送信すべきかを改めて知ることができる。

電子署名

電子署名リクエスト

B I A 部：

4 バイト B I A 識別

4 バイトシーケンス番号

暗号化された (D U K P T 鍵) バイオメトリック P I C ブロック：

3 0 0 バイト承認バイオメトリック

4 - 1 2 デジット P I C

5 6 ビットレスポンス鍵

文書名

文書 M D 5 計算

M A C

ターミナル部：(不使用)

電子署名レスポンス

暗号化 (レスポンス鍵)：

秘密コードテキスト

署名文字列

M A C

電子署名リクエストを処理するため、D P C はまず、バイオメトリック P I C を用いてバイオメトリック識別を行う。そして、D P C は E S D 記録を生成し、それに固有の署名識別コードを割り当て、記録の署名フィールドをそのリクエスト内の電子署名に設定する。そして D P C は、後の検証において提出されうる署名文字列を返す。

” <Dr. Bunsen HoneyDew> <Explosions in the Laboratory> 5/17/95 13:00 P
ST 950517000102”

電子署名検証

電子署名検証リクエスト

B I A 部：

4 バイト B I A 識別

4 バイトシーケンス番号

暗号化された（DUKPT鍵）バイオメトリックPICブロック：

300バイト承認バイオメトリック

4-12ディジットPIC

56ビットレスポンス鍵

署名文字列

MAC

ターミナル部：（不使用）

電子署名検証レスポンス

暗号化（レスポンス鍵）：

秘密コードテキスト

署名文字列

ステータス（検証済み、失敗）

MAC

DPCはバイオメトリック識別を行い、署名文字列から署名トラッキングコードを抽出し、示されたESD記録を取り出して、それが署名文字列に一致することを検証する。DPCは秘密コード及び署名の比較の結果を返す。

ネットワーククリデンシャル

ネットワーククリデンシャルリクエスト

BIA部：

4バイトBIA識別

4バイトシーケンス番号

暗号化された（DUKPT鍵）バイオメトリックPICブロック：

300バイト承認バイオメトリック

4-12ディジットPIC

56ビットレスポンス鍵

アカウントインデックス

銀行コード

銀行ホストネーム

ターミナルポート及び銀行ポート (TCP/IP アドレス)

MAC

ネットワーククリデンシャルレスポンス

暗号化 (レスポンス鍵) :

秘密コード

署名 (DPC秘密鍵) :

クリデンシャル (時間、アカウント、ターミナルポート、銀行ポート)

銀行公開鍵

ステータスコード (ok, 失敗)

MAC

DPCはリクエストのバイOMETリックPICを用いて個人を識別し、特定されたインデックスに格納された個人の資産のアカウントを取り出す。アカウントインデックスが緊急アカウントなら、ネットワーククリデンシャルレスポンスステータスコードは「失敗」と設定され、クリデンシャルは生成されない。

DPCは現在時間、取り出された資産アカウント、ターミナル及び銀行のTCP/IPアドレスを用いてクリデンシャルを作成する。そしてDPCは公開鍵暗号化を用いてその秘密鍵でクリデンシャルに署名する。レスポンスはまた、銀行のパブリック鍵を含むが、これはDPCが遠隔マーチャントデータベースから取り出したものである。

顧客サポート及びシステム管理メッセージ

DPCは内部メッセージに分類されるさらなるメッセージタイプを扱う。DPCは一般に、非DPCシステムからのこれらのメッセージを受け付けない。そのメッセージはデータベースベンダー特有である。しかし、内部ネットワークは更なるセキュリティのためDES暗号化パケットを用いている。

顧客サポート及びシステム管理タスクは、データベースベンダーの照会言語及びアプリケーション開発ツールを用いて実行される。

顧客サービスタスク

- ・IBD: 記録の検索、起動、終了、削除、訂正

- ・ A I D : 承認された個人の追加または、削除
- ・ A O D : 記録の検索、追加、削除、訂正
- ・ V A D : 記録の検索、起動、終了、削除、訂正
- ・ R M D : 記録の検索、追加、削除、訂正
- ・ P F D : 記録の追加、削除、訂正

システム管理タスク

- ・ 以前の詐欺チェックの実行
- ・ 有効なサイトリストの修正
- ・ ログ情報（警告、エラー等）の要約
- ・ P I C グループリストの修正
- ・ パフォーマンス監視
- ・ バックアップの実行
- ・ クラッシュ回復手続き
- ・ D P C サイトの時間同期化
- ・ 主要な登録サイトの変更
- ・ シークレット D E S 暗号鍵の変更

- ・ 古い文書トラッキング番号の削除

・ B I A ハードウェア識別コード、M A C 暗号化鍵及び、D U K P T ベース鍵の
三つ組みリスト生成。鍵読み込みデバイス用の暗号フロッピーへの格納。

ファイアウォールマシン

FWマシンは、ネットワークウイルスおよびコンピュータハッカーに対する第1線の防御を提供する。DPCサイトへの及びDPCサイトからのすべての通信リンクは、まず安全なFWマシンを通過する。インターネットローカルネットルータであるFWマシンは、GMマシン用のメッセージを取り扱うにすぎない。BIA搭載ターミナルは、モデム、X.25、または他の通信媒体を介して単一のDPCサイトにパケットを送信する。DPCは、第三者に依存して、呼の量を取り扱うため、およびDPCバックボーンへデータを供給するために必要なモデムバンクを供給する。

DPCからDPCへの通信、主に配布されたトランザクションおよびシーケンスナン

バの更新のために、FWマシンは、2倍の長さのDES暗号化パケットを送出する。DPC LANコンポーネントが、暗号化および復号化を取り扱い、FWは、パケットを復号化する能力を有していない。

適切に構成されたネットワークスニファ(sniffer)は、FW用のバックアップとしての侵入者検出器として作用する。変則的なメッセージが検出された場合、侵入するメッセージはその全体が記録されて、オペレータに警告が発され、FWはスニファにより物理的にシャットダウンされる。FWは、内部ネットワークからインターネットのそれ以外の部分への送信を禁止する。

トランザクション承認要求は約400バイトを必要とし、登録パケットは約2KBを必要とする。1秒あたり1000個のトランザクション承認および1秒あたり1個の登録パケットを扱うために、FWマシンは1秒あたり約400KBを処理する能力がある(すべては当該分野で知られている)。

各DPCサイトは、第三者のモデムバンクおよび他のDPCサイトへの3つのT1接続を総合した帯域幅を必要とする。

ゲートウェイマシン

GMマシン(GM)は、FWマシンを介して、外界(BIA搭載ターミナルおよび他のDP

C)をDPCの内部コンポーネントにリンクする。DPCは、複数、通常2つのGMを有する。

GMは、各BIA要求の処理を監督し、必要に応じて様々なDPCコンポーネントと通信し、要求の暗号化結果を送り手に送り返す。このタスクを行うソフトウェアは、メッセージプロセッシングモジュールと呼ばれる。

GMは、それが受け取るすべての要求、および通信するコンポーネントからのいずれの警告をも履歴に残す。例えば、GMは、いずれの緊急アカウントアクセス、シーケンスナンバギャップ、および無効パケットをも履歴に残す。要求の処理は、GMが、他のすべてのDPCにおけるGMに、DPCデータベース内の変更を通知することを必要とする。これが起こると、GMは、遠隔データベースを更新するために、配布されたトランザクションを行う。

配布されたトランザクションは、2つのカテゴリ、すなわち、同期および非同

期に分類される。同期配布されたトランザクションは、パケットの処理を続ける前に、配布されたトランザクションの送信に関する最終決定がなされることを、GMが待つことを必要とする。非同期配布されたトランザクションは、GMが最終決定がなされることを待つことを必要とせず、配布されたトランザクションの送信に関する最終決定がなされたか否かにかかわらずGMが要求の処理を終了することを許可する。非同期配布されたトランザクションは、データベースの一貫性が絶対に必要な事項ではないデータを更新するために用いられるのみである。シーケンスナンバおよびバイオメトリックチェックサム記録は、非同期に行われ得、他方、インディビジュアルバイオメトリック記録などのデータベース記録の作成は行われ得ない。

同期配布されたトランザクションを実行する場合に、すべてのサイトがローカルにトランザクションの送信に関する最終決定をすることに成功し得る場合、要求を出すGMは、トランザクション全体が成功したと考えるのみである。そうでない場合、GMは、ローカルに変更を取り消して、トランザクションエラーによる要求を拒否する。

有効なDPCサイトのリストは、通常全てのサイトである。しかし、極端なサイト障害(failure)の場合、システム管理者は、有効なサイトのリストからそのサイトを手動で除去し得る。しかし、配布されたトランザクションのフェイラの最も可能性の高い原因は、いずれのDPC装置とも無関係な一時的なネットワークフェイラである。同期配布されたトランザクションを必要とする要求は、ネットワークの接続可能性が回復されるか、またはサイトが有効サイトのリストから除去されるまで、行うことができない。サイトが有効なサイトのリストに再び追加されることができる前に、システム管理者は、サイトのデータベースを現在アクティブなサイトのデータベースまで更新する。

各GMは、性能上の理由で、ローカルに以下のソフトウェアを実行する。

メッセージプロセッシングモジュール

メッセージ認証コードモジュール

メッセージ復号化モジュール

インディビジュアルバイオメトリックデータベースマシンリスト

GMにより必要とされるメッセージの帯域幅は、FWマシンにより必要とされるものと同様である。FDDIネットワークインターフェースは、1秒あたり100Mビットを提供し、いずれの帯域幅の必要要件をも容易にカバーしている。

DPC LAN

DPCローカルエリアネットワーク(LAN)は、光ファイバトークンリングを用いて、DPCサイトのマシンを互いにリンクする。光ファイバトークンリングは、高域幅と良好な物理的安全性との両方を提供する。

DPC LAN上のマシンにより用いられるネットワークインターフェースは、暗号化鍵がない場合、パケットを盗み見ることまたは傍受することを無益にする暗号化ハードウェアを含む。暗号化鍵は、LAN上のすべてのマシン用のものと同一であり、暗号化ハードウェア内に格納される。

適切に構成されたネットワークスニファは、FW用のバックアップとしての侵入者検出器として作用する。変則的なメッセージが検出された場合、侵入するメッセージはその全体が記録されて、オペレータに警告が発され、FWはスニファにより物理的にシャットダウンされる。

メッセージプロセッシングモジュール

メッセージプロセッシングモジュール(MPM)は、要求パケット用の処理を扱う。M

PMは、そのタスクを実行するために必要に応じてDPCの他のコンポーネントと通信する。マシン上にMPMが存在することにより、マシンはGMと呼ばれる。

MPMは、現在処理中の各要求の要求コンテキストを維持する。要求コンテキストは、要求を行っているターミナルに対するネットワーク接続を維持するために必要な情報、BIAデバイス情報、レスポンス鍵、およびレスポンスパケットを含む。

メッセージ認証コードモジュール

メッセージ認証コードモジュール(MACM)タスクは、送られてくるパケット上のメッセージ認証コードの有効性を証明すること、および送出されるパケットにメッセージ認証コードを付加することである。MACMは、BIAハードウェア識別コー

ドにより鍵をかけられた112ビットのMAC暗号化鍵のメモリ内ハッシュテーブルを維持する。

MACMは、パケットのMACの有効性を証明するようにという要求をGMから受け取ると、まずハッシュテーブル内のパケットのハードウェア識別コードを参照する。エントリがない場合、MACMはGMに「無効なハードウェア識別コード」エラーであると応答する。

そうでない場合、MACMは、112ビットの暗号化鍵を用いて、パケットのBIAメッセージ部のMACチェックを行う。MACチェックが失敗した場合、MACMはGMに、「無効なMAC」エラーであると応答する。そうでない場合、MACMは、「有効なMAC」メッセージであると応答する。

パケットがマーチャントコードを含む場合、MACMはさらに、ハッシュテーブル内のオーナー識別コードに照らしてマーチャントコードをチェックする。コードが合致しない場合、MACMは「無効なオーナー」エラーであると応答する。

MACMは、パケット用のMACを生成するようにという要求をGMから受け取ると、パケットのハードウェア識別コードを用いてMAC暗号化鍵を参照する。MACMは、MAC暗号化鍵で、MACを生成してパケットに付加する。MACMがハードウェア識別コードを見つけることができない場合、MACMは、代わりに、無効なハードウェア識別コードエラーであると応答する。

MAMCハッシュテーブルエントリは、以下を含む。

MACMエントリ：

hardwareID=int4

ownerID=int4

macEncryptionKey=int16

テーブルは、ハードウェア識別コードによりハッシュされる。

500万のBIA搭載デバイスがサービスを行っているとすると、ハッシュテーブルは、約120MBの記憶容量を必要とする。性能上の理由により、このハッシュテーブルは、メモリ内で完全にキャッシュされる。

MACMは、アクティブなBIAハードウェア識別コードおよびアクティブな装置オ

ーナを参照する記録を含むのみである。装置または装置オーナーが一時使用不可能にされるか、またはシステムから削除される毎に、MACMはその識別コードを参照するエントリを除去する。装置がアクティベートされると、MACMはその装置用のエントリを追加する。

MAMCはまた、有効な装置データベースからMAC暗号化鍵をキャッシュする。システムはBIAの暗号化鍵が変更されることを許可しないため、MACMは暗号化鍵の更新を受け取ることに對して懸念する必要はない。

メッセージ復号化モジュール

メッセージ復号化モジュール(MDM)タスクは、DUKPTトランザクション鍵を再構築すること、およびそれによりパケットのバイオメトリックPICブロックを復号化することである。メッセージ復号モジュール(MDM)は、トランザクション鍵を生成するために必要なDUKPTベース鍵のリストを維持する。

MDMは、DUKPTトランザクションカウンタとしてのパケットのシーケンスナンバ、DUKPT不正改変不可能な安全なモジュール(すなわち「TRSM」)識別子としてのBIAハードウェア識別コードの上位22ビット、およびDUKPT鍵セット識別子としてのBIAハードウェア識別コードの下位10ビットを用いて、DUKPTトランザクション鍵を再構築する。

DUKPT標準は、トランザクション鍵がどのように生成されるかを特定する。鍵セット識別子は、ベース鍵リストからベース鍵を参照するために用いられる。ベース鍵は、DES暗号化／復号化／暗号化のサイクルを介して、TRSM識別子を初期

鍵に変換するために用いられる。その後、トランザクションカウンタは、一連のDES暗号化／復号化／暗号化のサイクルとしての初期鍵を、トランザクション鍵を生成するために適用するために用いられる。

更なる安全性のために、2つのベース鍵リストが維持される。1つは低安全性BIAデバイス用であり、1つは高安全性デバイス用である。MDMは、デバイスの安全性レベルに応じて、いずれのベース鍵を用いるかを選択する。

MDMベース鍵リストエントリは、以下を含む。

MDMエントリ：

baseKey : int16

ベース鍵リストは、鍵セット識別子によりインデックスを付けられる。

MDMは、DUKPTベース鍵のメモリ内リストを維持する。各鍵は、112ビットを必要とする。MDMは、1024鍵を2組必要とし、合計32KBを必要とする。MDMは、他のいずれのDPCコンポーネントにも直接依存しない。

PICグループリスト

PICグループリスト(PGL)は、インディビジュアルバイオメトリックデータベースマシンリストと共に、IBDマシンの構成を定義する。PGLは、PICの管理を簡素化するために用いられるシステム内にPICグループのリストを格納する。PICグループは、一連の連続したPICコードである。PGLは、各GMマシン(GM)上に存在する。

PGLは、PICコードを与えられると、上記PICコードを含むグループを見つけるためにPICグループのリストをサーチする。PGLはグループのリストを順序立てて維持し、正しいグループを迅速に見つけるためにバイナリサーチを用いる。

PGLの初期構成は、全ての可能性のあるPICを含む1つの巨大なPICグループである。PICの閾値ナンバが割り当てられた後、巨大なPICグループは2つに分割される。その後、このプロセスが全てのPICグループに適用される。

PICグループが分割されると、PGLは、早いものからサーブする(first-come-first serve)様式で入手可能な記憶容量に基づいて、新しいメインおよびバックアップIBDマシンを割り当てる。PGLは、IBDマシンと協力して、まず、影響を受ける記録を古いメインおよびバックアップマシンから新しいものにコピーし、IML記録を更新し、最後に古いメインおよびバックアップコピーを除去する。PICグ

ループを分割することは、複雑なタスクである。PGLバッチは、DPCのロードが軽いつき、例えば夜に実行されるように、要求を分割する。

システム管理者はさらに、マシンのフリーな記憶容量が予測された量の新しい登録を取り扱うために要するレベルを下回る場合、与えられたPICグループ用のメインおよびバックアップIBDマシンを変更し得る。

PICグループ記録用のスキーマは以下の通りである。

PICグループ：

lowPin=int8

highPin=int8

used=int4

各PICグループは、固有の識別子により識別される。便宜上、PICグループ識別コードをグループ用のlowPinコードとするが、そうでない場合システムはこの事実には依存しない。PGLはlowPinフィールドにより鍵をかけられる。

PGLグループは、約3000グループを含むと予測される（各PICグループは約1000のアクティブなPICを含むが、数百万の実際のPICをカバーし得る）。PGL全体は、約72KBの記憶容量を要し、メモリ内で完全にキャッシュされる。

PICグループが追加、マージ、または分割されると、PGLはIBDマシンリストに変更を通知し且つ1つのIBDマシンから別のIBDマシンへのIBD記録の移動を指示する責任がある。

インディビジュアルバイオメトリックデータベースマシンリスト

IBDマシンリスト(IML)は、PICグループリストと共に、IBDマシンの構成を分類する。IMLは、PICコードを、PIC用のIBD記録を格納するメインおよびバックアップIBDマシンにマッピングする。IMLは実際、個々のPICではなくPICグループ（連続したPICコードのセット）により鍵をかけられる。なぜなら、この方が、リストを格納するために要するメモリが減少するからである。IMLは各GMマシン(GM)上に存在する。

GMがバイオメトリック識別子を必要とする要求を処理すると、GMは、バイオメトリックのPICグループにより鍵をかけられたIML記録を見つける。そうすると、GMは、バイオメトリック識別子用に用いるべきメインおよびバックアップIBDマ

シンを知る。

IMLリストエントリ用のスキーマは以下の通りである。

マシンペア：

pinGroup=int8

main=int2

backup=int2

IMLはpinGroupにより鍵をかけられる。

IMLは、約3000のエントリ（PICグループの数）を含むと予測される。各マシンペア記録は12バイトであって約36KBの記憶容量を要し、メモリ内に完全にキャッシュされる。IBDマシンの構成のいずれの変更もが、IMLに反映されることになる。更に、IMLは、PICグループリストが改変されるとIMLもまた更新されるように、鍵用にPICグループを用いる。

シーケンスナンバモジュール

シーケンスナンバモジュール(SNM)の主要な機能は、パケットのシーケンスナンバの有効性を証明することによりレプレイ攻撃を防ぐことである。その二次的なタスクは、遠隔DPCサイトの他のSNMにシーケンスナンバの更新を通知することにより再入力攻撃の影響を最小にすること、および有効な装置データベース内のシーケンスナンバを定期的に更新することである。SNMは、BIAハードウェア識別コードによって鍵をかけられたシーケンスナンバのメモリ内ハッシュテーブルを維持して、パケットシーケンスナンバの迅速な有効性証明を可能にする。

SNMは、与えられたハードウェア識別コードとシーケンスナンバに対する有効性証明要求をGMから受け取ると、ハッシュテーブル内のハードウェア識別コードを参照する。エントリが存在しない場合、SNMはGMに「無効なハードウェア識別コード」エラーであると応答する。

そうでない場合、SNMは、ハッシュテーブルエントリ内に格納されたシーケンスナンバに照らして与えられたシーケンスナンバをチェックする。シーケンスナンバが格納されたシーケンスナンバ以下である場合、SNMは「無効なシーケンスナンバ」エラーであると応答する。そうでない場合、SNMは、ハッシュテーブルエントリ内のシーケンスナンバを、上記与えられたシーケンスナンバに設定して、

「有効なシーケンスナンバ」メッセージであると応答する。

SNMはしばしばシーケンスナンバギャップを観察し得る。シーケンスナンバギャップは、SNMがハッシュテーブルエントリ内に格納されたシーケンスナンバよ

りも1を越えた分だけ大きいシーケンスナンバを受け取るときに起こる。換言すると、シーケンスナンバはスキップされた。

SNMは、シーケンスナンバギャップを発見すると、「有効なシーケンスナンバ」メッセージに代えて「シーケンスナンバギャップ」メッセージであるとGMに応答する。GMは、パケットを有効なものとして扱うが、また「シーケンスナンバギャップ」警告を履歴に残す。

シーケンスナンバギャップは通常、ネットワーク接続可能性が失われたとき、例えば、パケットがドロップしたり、あるいはネットワークが回復して作動するまで送信できないときに起こる。しかし、シーケンスナンバギャップは、詐欺的な理由によっても起こる。悪意のある者が、パケットを傍受してDPCに到着することを妨げる、あるいは、パケットを偽造することさえあり得る（すぐに拒否されないように大きなシーケンスナンバで）。

SNMの二次的機能は、更新されたシーケンスナンバを他のDPCに通知することである。すべてのDPCサイトにおいてシーケンスナンバを迅速に更新することは、悪意のある者が1つのDPCサイトに向けられたパケットをモニタして、1つのDPCサイトから別のDPCサイトへのシーケンスナンバ更新の送信遅延を利用することを期待して即刻異なるDPCサイトにコピーを送り、その結果、第1のサイトのみがパケットを受け入れるべきときに両方のサイトがパケットを有効なものとして受け入れるという、再入力攻撃を防ぐ。

SNMは、有効なシーケンスナンバを受け取る毎に更新メッセージを互いに送信し合う。SNMは、ハッシュテーブル内に現在格納されているシーケンスナンバ以下のシーケンスナンバへの更新メッセージを受け取った場合、シーケンスナンバ再入力警告を履歴に残す。すべての再入力攻撃はこのようにして検出される。

再入力攻撃を完全に防ぐ、より簡単な方法は、1つのSNMのみにパケットの有効性を証明させることである。このスキームの場合、再入力攻撃で利用される更新遅延ウィンドウはない。あるいは、同一のBIA搭載デバイス用のシーケンスナ

ンバの有効性の証明を取り扱うSNMがない場合、複数のSNMが同時にアクティブになり得る。

SNMは、ブートアップすると、VAD内に格納されたアクティブなBIA用のシーケンスナンバから、シーケンスナンバハッシュテーブルをロードする。SNMは、1日に1度、現在のシーケンスナンバを、ローカルな有効装置データベース(VAD)にダウンロードする。

VADは、SNMハッシュテーブルを最新の状態に維持するためにアクティベートまたはディアクティベートされるいずれのBIA搭載デバイスに対しても、エントリ追加およびエントリ除去メッセージをSNMに送信する責任を有する。

SNMハッシュテーブルエントリは、以下を含む。

SNMエントリ：

hardwareID=int4

sequenceNumber=int4

ハッシュテーブルは、hardwareIDによって鍵をかけられる。

約500万のBIA搭載デバイスがサービスを行っているとすると、約40MBのハッシュテーブルが必要である。

SNMは、有効な装置データベースに依存する。装置が一時使用不可能にされるかデータベースから除去されると、SNMは対応するエントリを除去する。装置がアクティベートされると、SNMはそのためのエントリを作成する。

SNMは、1秒あたり1000の更新シーケンスナンバメッセージを処理するために1秒あたり約8KBの送信帯域幅を必要とする。更新シーケンスナンバメッセージは、実際に送られるメッセージの数を最小にするために、バッファに保持されて1秒に1度送出される。

発行者データベース

発行者データベース（ID）は、システムを通じてその資産アカウントへのアクセスが許される銀行及び他の金融機関についての情報を格納している。発行機関は、資産アカウント番号を、与えられた個人のIBD記録に追加したりそこから除去したりできる、唯一の存在である。

DPICは、IDを使用して、発行者ターミナルの発行者コードを含む記録を求めてIDをサーチすることによって、発行者ターミナルからのリクエストの有効

性を検査する。記録に格納された所有者の識別子は、発行者ターミナルに記録された B I A のための有効装置データベースに格納された所有者と、一致しなければならない。

発行者記録のためのスキーマは、
発行者記録：

```
issuerCode=int6  
ownerId=int4  
name=char50  
phoneNumber=char12  
address=char50  
zipCode=char9
```

である。

発行者データベースは、issuerCodeによって鍵をかけられる。

発行者データベースは、約100,000のエントリを取り扱う。各々のエントリは、2MBより少なく要求する127バイトである。IDのコピーが、各々のGMに格納される。

発行者データベースは、他の何れのDPCコンポーネントにも、直接の依存性を有さない。

電子文書データベース

電子文書データベース（EDD）は、特定の個人に向けられたファックスイメージや電子メールメッセージのような電子文書を格納し、且つトラックする。それはまた、会社組織のチャートを維持して、送り手及び受け手の両方の公式な肩書きを提供する。EDDはまた、送り手或いは受け手のリクエストに応じて文書をアーカイブし、システムを通じて提出された契約同意事項に、中立の第3者の検証を与える。

DPCは、個人からファックス或いは他の電子文書を受領すると、EDD文書記録を生成して、承認された受け手によってピックアップされるまで、その文書を格納する。

ファックス文書に関しては、受け手は、ファックス番号及び内線によって特定される。他の電子文書に関しては、受け手は、電子メールアドレスによって特定される。D P Cは、ファックス番号及び内線或いはeメールアドレスによって個々の受け手を求めて、組織記録を調べる。もし、記録が発見されないと、D P Cは次に、受け手がeメールアドレスによって特定されるときにのみ、個人バイオメトリック記録を見る。個々の受け手に関して、D P Cは、文書、及び、もし発見された場合には組織或いはI B D記録によって特定された受け手のバイオメトリック識別子、の両方を参照する受け手記録を生成する。D P Cは、システムに登録されていない受け手を許容するが、そのときにはD P Cは、これらの受け手に対する配達或いは機密性を保証できない。

E D Dは、十分にフレキシブルであって、ファックス文書が個人のeメールアドレスに送られたり、eメールメッセージがファックス番号に送られることを、許容する。

文書上にシステムによって電子署名が置かれていない間は、システムは、証明されたEメール或いはセキュリティファックスターミナルによって受領（或いは復号）されたメッセージが個人によって送られたことを、暗号化を通じて保証する。

組織の正式に承認されたオフィサーは、D P Cへのファックス或いは電子メッセージへの肩書きの割り当て及びファックス番号への内線の割り当て、メンバの肩書きやファックス番号の更新、或いは、いなくなったメンバの削除、を確実に行う。

個人が組織のツリーから削除されると、D P Cは、内線番号を1年間引き上げる。この引き上げ期間は、その内線番号でのコンフィデンシャルファックスを彼がもはや受領することができず、従って、その内線において、彼或いは彼女を意図していないファックスを受領し得る可能性がある他の誰かを組織が誤ってアクティベートすることがない旨を、コンフィダントに伝えるための個別の十分な時間を許容する。

E D Dは、文書の送り手或いは受け手の一人によってリクエストされたときに

、文書及び受け手記録のコピーを含むアーカイブデータベースを維持する。アーカイブデータベースは、CD-ROMの上に定期的に移動される。

E D Dは、3つの記録タイプを有する：

文書記録：

```
documentNumber=int8  
senderId=int4  
documentFax=fax  
documentText=text  
messageKey=int8  
status=int1
```

受け手記録：

```
documentNumber=int8  
recipientId=int4  
recipientFaxNumber=char12  
recipientFaxExtension=char8  
recipientEmailAddr=text  
receivedBy=int4  
lastModified=time  
deliveryStatus=int1  
contactStatus=int1
```

アーカイブリクエスト記録：

```
biometricId=int4  
documentNumber=int8  
requestorFaxNumber=char12  
requestorFaxExtension=char8  
  
requestorEmailAddr=text
```

組織記録：

```
biometricId=int4
```

registeredBy=int4
company=text
title=text
faxNumber=char12
faxExtension=char8
emailAddr=text
activeDate=time
priv=int2
status=int1

文書記録ステータスフィールドは、

- 0 : incomplete
- 1 : ok

の一つである。

受け手記録デリバリステータスフィールドは、

- 0 : incomplete
- 1 : notified
- 2 : rejected
- 3 : retrieved
- 4 : retrieved unsecured
- 5 : busy

の一つである。

受け手記録コントラクトステータスフィールドは、

- 0 : none
- 1 : accepted

- 2 : rejected

の一つである。

組織記録ステータスフィールドは、

- 0 : active

1 : suspended

の一つである。

組織記録privsフィールドは、D P Cがその個人にどの特権を許容するかを示すために使用される。

0 : registration

文書、受け手、及びアーカイブ取り出し記録は、documentNumberによって鍵をかけられる。組織記録は、biometricIdによって鍵をかけられる。E D Dは、文書のsenderIdフィールド、受け手のrecipientIdフィールド、及び組織の会社名及び肩書きフィールドに、副インデックスを維持する。

E D Dのストレージ要求は、主として、それが格納しなければならないファックスのページ数に依存する。なぜなら、eメールメッセージは、ファックスページに比べて比較的小さいからである。各々のファックスページは、約110KBのストレージを必要とする。1つのファックス毎に4ページ、一人一日当たり2つのファックスであって、3千万台のファックス機があるとするれば、E D Dは、1日分のファックスをスプールするために、24GBのストレージを必要とする。

文書は、B I A暗号化メカニズムを使用して、暗号化されたシステムへ、及びそこから、送られる。しかし、暗号化の鍵は、文書と同じデータベースに格納されている。文書は、偶然の開示を防ぐために、暗号化された形式で残される。しかし、システムに格納された文書のセキュリティに関心がある個人は、付加的な暗号化それ自身のために、何らかのアレンジメントを行う。

各々のファックスページは約110KBを必要とし、そのことは、1.54Mbits／秒のスループットを有するT1接続が、1秒当たり1.75ファックスページを取り扱えることを意味している。

電子署名データベース

電子署名データベースは、システムによって生成された全ての電子署名を認証してトラックする。

システムのメンバである個人は、バイオメトリックP I Cとともに文書に関する16バイトの「メッセージダイジェスト」を提出して、永久にシステムにおけ

るファイル上に残る「デジタル署名」を得る。このデジタル署名は、個人の名前、バイオメトリック識別子、承認された署名記録番号、文書のタイトルを、文書が署名された時刻印とともにコード化する。

署名を検証するために、文書に関するメッセージダイジェストが（例えばRSAのMD5を使用して）最初に計算されて、文書の署名タグと共に送られる。ESDは、署名タグを調べて、データベースに格納されたメッセージダイジェストに対して、つい最近計算されたメッセージダイジェストの有効性を検査する。

電子署名のためのスキーマは、

電子署名：

```
signatureNumber=int8  
signer=int4  
documentName=text  
checksum=int16  
date=time
```

である。

署名者は、文書に署名する個人に対するバイオメトリック識別コードである。

電子署名記録は、signatureNumberによってハッシュされる。

1GBの副ストレージ毎に、電子署名データベースは、2700万の記録（各記録は約32バイト）を格納する。

ESDは、署名者のバイオメトリック識別子に対する依存性を有する。これらの署名は、本質的に永久に有効であるので、ESD記録は、システムが署名者の個人バイオメトリック記録を削除するときに、除去されない。これは、IBDがバイオメトリック識別子を決して再利用しないことを必要とする旨に、留意されたい。

リモートマーチャントデータベース

リモートマーチャントデータベース（RMD）は、電話、ケーブルテレビネットワーク、或いはインターネットを通じて商品やサービスを提供するマーチャントに関する情報を格納する。適切に備えられたターミナルを使用して個人によっ

て送られた各オーダは、マーチャントのオーダターミナルを通じてシステムにルートされる。

個人のリモートトランザクションの承認がDPCによって受領され、且つMACの有効性が検査されると、マーチャントコードがRMDのマーチャントコードと比較される。マーチャントコードは、それが電話番号、マーチャントー製品クレデンシャル、或いはインターネットアドレスであれば、RMD記録の中において、正しいマーチャント識別コードの下に存在し、そうでなければ、DPCターミナルがリクエストを終了して、無効なマーチャントコードエラーを送り手のBIAターミナルデバイスに送り返す。

リモートマーチャント記録のためのスキーマは、

リモートマーチャント：

```
merchantId=int4  
merchantCode=char16  
merchantType=int1  
publicKey=int16
```

である。

リモートマーチャントのmerchantTypeは、

```
0 : telephone  
1 : C A T V  
2 : Internet
```

の一つである。

merchantId及びmerchantCodeは、どちらも主要な鍵である。2つのRMD記録が同じmerchantId及びmerchantCodeの組合せを有することはない。

約100,000のリモートマーチャントが存在するとすれば、RMDは、必要とされる約2.4MBのストレージの総量のために、1記録当たり約24バイトを必要と

する。RMDは、他のDPCコンポーネントの何れに対しても直接の依存性を有さない。

システムのパフォーマンス

鍵となるパフォーマンス数は、DPCが1秒当たりいくつの金融承認トランザクションを取り扱えるかである。

GMにおいて：

1. MACMがMACをチェックする（ローカル）
2. SNMがシーケンス番号をチェックする（ネットワークメッセージ）
3. MDMがバイオメトリックPICブロックを復号する（ローカル）
4. IBDマシンを見つける（ローカル）
5. 識別リクエストをIBDマシンに送る（ネットワークメッセージ）

IBDマシンにおいて：

6. PICのための全てのIBD記録を取り出す（xがバイオメトリック記録を格納するために必要とされるページ数であるときに、x回のシーク及びx回の読み出し）

7. 各記録毎に、その主バイオメトリックに対して比較する（yが取り出された記録数であるときに、 $y/2ms$ ）

8. 適切なマッチングがなければ、ステップ9を繰り返すが、副バイオメトリックに対して比較する（yが取り出された記録数であり、zがマッチングが発見されない確率であるときに、 $z \times y/2ms$ ）

9. ベストマッチングのIBD記録のチェックサム列を更新して、可能性のあるリプレイアタックをチェックする（1回のシーク、1回の読み出し、及び1回の書き込み）

10. ベストマッチングのIBD記録、或いはみしマッチングが十分に近くないときにはエラーを、戻す（ネットワークメッセージ）

GMにおいて：

11. 外部プロセッサでリクエストを承認する（ネットワークメッセージ）
12. GMがレスポンスを暗号化してMACする（ローカル）
13. レスポンスパケットを送り返す（ネットワークメッセージ）

全ディスクコスト：

$$x \times (s + r) + y/2 \times (1 + z) + s + r + w + 5 \times n$$

$$= (x + 1) \times s (+) r_y + \times 2(1) + z + 5 \times w + n$$

(1) [xが20あり、y、kが3あり、zが5あり、sが10ms、r

s、w=0ms、n=0msあるとすれば

$$= 2 \times 10 \text{ ms} + 1055 \text{ ml s}$$

$$= 226 \text{ sm}$$

$$= 4.4 \text{ T P S}$$

[xが10あり、y、kが5あり、zが5あり、sが10ms、n

s、w=0ms、n=msあるとすれば

$$= 1 \times 10 \text{ ms} + 705 \text{ ml s}$$

$$= 118 \text{ sm}$$

$$= 8.4 \text{ T P S}$$

[xが1あり、y、kが1あり、zが5あり、sが10ms、n

w=0ms、n=msあるとすれば

$$= 2 \times 10 \text{ ms} + 051 \text{ ml s}$$

$$= 21 \text{ ms}$$

$$= 47 \text{ T P S}$$

バックアップIBDマシンが、やはり2重に有効なTPSをリクエストする。

最悪のケース（2つのマシンが使用されている）：

Individuals/PIC T P S

30 8

15 16

1 94

平均のケース（20のマシンが使用されている）：

Individuals/PIC T P S

30 88

15 168

1 940

最良のケース（40のマシンが使用されている）：

Individuals/PIC	T P S
3 0	1 7 6
1 5	3 3 6
1	1 8 8 0

上記は、商業的に存立し得る方法によって実行可能なシステムのある構成の、単なる一例である。しかし、本発明が、より速いコンピュータ、より多くのコンピュータ、及び他のそのような変化を盛り込み得る他の多くの方法によって構成され得ることが、期待される。

ターミナルプロトコルフローチャート

以下のプロトコルフローのセットは、特定のターミナル、D P C、付属されたB I A、及びクレジット／デビットプロセッサなどの他の関係者の間でのやりとりを記述する。

小売P O Sターミナル

この場合、R P Tターミナルは、小売B I A及びD P Cと通信して、トランザクションを承認する。トランザクション量は452.33であって、個人のアカウント

は4024-2256-5521-1212であって、マーチャントコードは123456であって、個人のプライベートコードは「私はそれを完全に確信している」である。

RPT → BIA set Language <英語>

BIA → RPT Ok

RPT → BIA Get Biometric <2 0>

BIA/LCD: <明るくされたパネルに指を置いて下さい>

個人がスキャナに指を置く

BIA → RPT Ok

RPT → BIA Get Pin <4 0>

BIA/LCD: <あなたのP I Cを入力し、その後に<enter>を押して下さい>

個人がP I Cを入力し、その後に<enter>する

BIA → RPT Ok

RPT → BIA Get Account Number <40>

BIA/LCD: <あなたのアカウントインデックスコードを入力し、その後に
<enter>を押して下さい>

個人がコードを入力し、その後に <enter> する

BIA → RPT Ok

RPT → BIA Validate Amount <452.33> <40>

BIA/LCD: <452.33という量はOK?>

個人がOKを入力する

BIA → RPT Ok

装置オーナーデータベース

装置オーナーデータベース (AOD) は、BIA-装備の装置を所有する個人または組織の情報を蓄積する。この情報は、金融上の貸方と借方のトランザクションのための資産アカウント情報を提供し、そして特定の個人または組織が所有する全てのBIAの識別を可能にするために、BIA装置は正当なオーナーによ

ってのみ使用されるということの、2重のチェックを行うために使用される。

DPCが、オーナーのBIA-装備の装置の1つにより寄託される金融上のトランザクションを処理する時、各々のAODレコードは、オーナーの貸方と借方の資産アカウントを含む。例えば、販売拠点の小売り地点に取り付けられたBIAから寄託されたトランザクションは、資産アカウントに対する貸方を含み、一方、認可された電子郵便トランザクションは資産アカウントの借方となる。

装置オーナーのレコードの概要は

装置のオーナー:

ownerId=int 4

name=char 50

address=char 50

ZipCode=char 9

assetAccont=char 16

status=int 1

ステータス領域の1つは：

0：停止

1：動作

装置オーナーデータベースは、オーナー I d によって鍵がかかる。

A O D は、約 2 百万の装置オーナーレコードを記憶すると予想される。約 2 6 0 M B の記憶領域を必要とする。各エントリは 1 3 0 バイトとなる。A O D は、オーナー識別コードによって鍵がかかるハッシュドファイルとして記憶される。A O D のコピーは各々の G M に蓄えられる。

登録が A O D から削除または停止される時、これらの装置オーナーを参照するいかなる正当なデータベース装置記録も停止としてマークされる。さらに、M A C モジュールとシーケンスナンバーモジュールは停止された装置に対するそれらの登録を削除する。

正当な装置のデータベース

正当な装置のデータベース（V A D）は、現在までに製造された B I A の全てを表す記録の集大成である。B I A が作動しているか、送信待ちか、または破壊されたとしてマークされているかの表示と共に、V A D 記録は、各 B I A のためのメッセージ認証コードの暗号化鍵を持っている。B I A からのメッセージを復号化するためには、B I A が存在して V A D 内にアクティブなレコードを持たなければならない。

製造時、各々の B I A は固有の公開識別コードと固有の M A C の暗号化鍵とを有し、これらは共に B I A の展開の前に V A D レコードに入れられる。

B I A は最初に構成される時、固有のハードウェア識別コードを与えられる。B I A が使用される時、そのハードウェア識別コードはシステムにおいて登録される。最初、そのオーナーもしくは B I A の信用できる団体は装置オーナーデータベース（A O D）の中に入れられる。次に、V A D レコードは、A O D 記録にポイントされ、そして B I A は、アクティブにセットされる。B I A からの要求は D P C によって受け入れられる。

B I A は使用から除外される時は、非アクティブとしてマークされ、そして A

OD記録へのリンクは壊される。B I Aからの通信は受け入れられない。

各B I Aタイプおよびモデルには、物理上のセキュリティレベルであるセキュリティレベルが割り当てられている。D P Cは、そのB I Aからの要求を処理する時、どの種類の動作が許可されるかを判定するためにB I Aのセキュリティレベルを使用する。D P Cは、また外部の金融トランザクション認証サービスにセキュリティレベルを提供する。

認証サービスも、リスクに基づいてトランザクションのためにどれほどチャージするかガイドとしてセキュリティレベルを使用できる。セキュリティレベルとそれらが許可する動作は、操作において決定される。

正当な装置のレコードの概要は

正当な装置：

hardwareId=int 4

macEncryptionKey=int 1 6

ownerId=int 8

mfgDate=time

inServiceDate=time

securityLevel=int 2

status=int 1

type=int 1

use=int 1

ステータスフィールドの可能な数値は：

0：停止

1：動作（アクティブ）

2：破壊

タイプフィールドの可能な数値は（各ターミナルタイプに対して1つ）：

0：A T M

1：B R T

2：C E T

3 : C P T

4 : C S T

5 : E S T

6 : I P T

7 : I T

8 : I T T

9 : P P T

10 : R P T

11 : S F T

使用フィールドの可能な数値は：

0 : リテイル

1 : 個人

2 : 発行人

3 : 遠隔

正当な装置のデータベースはハードウェアの識別コードによって鍵がかかる。

V A Dは約5百万のリテイル、発行人、および遠隔の正当な装置エントリを扱う。各エントリは51バイトとなり、合計約255MBを必要とする。V A Dは、ハードウェア識別コードによって鍵がかかるハッシュドファイルとして記憶される。V A Dのコピーは各GM上に記憶される。

個人的な正当な装置エントリ数は、3千万の範囲であり、1.5MBの記憶領域を必要とする。

V A Dレコードがステータスが変わる時、M A Cモジュールおよびシーケンスナンバーモジュールは、そのステータスの変化について通知される。例えば、装置がアダプティブになると、M A C P及びS N Mは、新しくアダプティブとなった装置のエントリを追加する。装置が非アダプティブになると、M A C P及びS N Mは、その装置のエントリを削除する。

個人バイオメトリックデータベース

個人バイオメトリックデータベース (I B D) レコードは個人の情報を記憶し

、それらは、1 次的、2 次的なバイオメトリック、P I C コード、金融資産アカウントのリスト、プライベートコード、緊急アカウント、アドレス、そして電話番号を含む。個人は、これらの S S N と電子メールアドレスを選択的に持っている。この情報は、バイオメトリックか個人情報のどちらかによって個人を識別するか、アカウントの情報にアクセスするか、または追加された検証のためアドレスまたは電話番号を遠隔のトランザクション者に提供するために必要である。

世界規模のリテイル銀行組織内で、またはローカルシステムオフィス内に位置する登録されたバイオメトリック登録ターミナルでの個人記録プロセスの間に、個人はシステムに追加される。登録の間、個人は、その個人識別ナンバーを選択

し、そして、そのバイオメトリックと P I C コとの組み合わせに金融資産アカウントを追加する。

個人は、発行ナンバーによって不正活動が報告されると、データベースから削除され得る。これが起こると、認可された内部システムの代表によって、個人のアカウント情報は I B D から以前の詐欺データベース (P F D) に移動される。P F D 内のレコードのためのバイオメトリック I d は I B D 内のレコードのために使用されない。

その I B D は、複数の装置に存在し、各々の装置は、過剰と負荷分担の両方に対して、2 つの異なる装置に記憶された各レコードのコピーと共に I B D レコードの下位集合に責任がある。

個人バイオメトリックレコードの概要は：

個人バイオメトリック：

```
primaryBiometric=Biometric  
secondaryBiometric=Biometric  
BiometricId=int 4  
P I C =char 1 0  
phoneNumber=char 1 2  
lastName=char 2 4  
firstName=char 2 4
```



```
middleInitial=char 2  
SSN=char 9  
privateCode=char 4 0  
address=char 5 0  
ZipCode=char 9  
publicKey=char 6 4  
checksums=int 4 [1 0]  
acctLinks=char 3 0 [1 0]  
emergencyIndex=char 1
```

```
emergencyLink=char 1  
privs=char 1 0  
enroller=int 8  
emergencyUseCount=int 4  
status=int 1
```

ステータスフィールドは次の1つ：

- 0：停止
- 1：動作
- 2：以前の詐欺

I B DはP I Cによって鍵がかけられる。

各々のI B D装置は、I B Dへのアクセスを容易にするため、個人のセキュリティナンバー、バイオメトリック識別コード、ラストネーム、ファーストネーム、そして電話番号について付加的なインデックスを持っている

各I B D装置は1つ以上のR A I Dデバイスによって提供される40MBの2次記憶装置を持っている。各々のI B Dレコードは、バイオメトリックが各々1Kと仮定すると2658バイトであり、装置あたり15百万レコードまで可能である。I B Dレコードは、P I C上の（おそらく群状の）2次インデックスを使って記憶される。インデックスはメモリーに記憶され、64MB（64MBインデックスは約16百万のエントリを扱う）しか必要としない。3億の個人のため

のレコードを記憶するためには、D P Cは、少なくとも40のI B D装置が、主記憶装置として20個のI B D装置およびバックアップとしてさらに20個が必要となる。

I B D装置の数は、登録される個人の数によって容易に増減される。

I B D装置、P I Cグループリスト、そしてI B D装置リストは、どのP I Cがどの装置上のあるのかによって、最新のもので残される。P I Cグループが再構成されるか、またはP I Cグループのメインとバックアップが変わる時、I B D装置は、これらのデータベースとインデックスを適切に更新する。

承認された個人データベース

各々の発行人または個人のB I A装備デバイスに対して、認可された個人データベース（A I D）は、デバイスのオーナーによって使用が承認された個人のリストを保持する。

A I Dは次の2つの理由のために存在する。その第一理由はターミナルに限されたアクセスを提供することである。例えば、発行人のターミナルは、承認された銀行の代表によってのみ使用され得る。A I Dの第2の理由は、犯罪者が電話ターミナルの個人のB I Aに秘密裏に置き換え、リテイルP O SターミナルのB I Aを販売拠点のリテイル点において、すべての購入物を犯罪者によって設定された遠隔のトランザクション者のアカウントに仕向けるのを防ぐことである。

承認された個人のレコードの概要は：

承認された個人：

hardwareId=int 4

biometricId=int 4

Hardware I dは、正当な装置のデータベースにおけるレコードを意味し、そしてbiometric I dは、個人のバイオメトリックデータベースを意味する。

D P Cは、個人が個人または発行人B I Aデバイスを利用することが承認されるかどうかのチェックが必要なときはいつでも、D P Cは、正しいHardware I dとbiometric I dとを持つ承認された個人レコードの存在をチェックする。

個人B I Aデバイスは、正当な装置のデータベースにおいて1（個人）に設定

された使用フィールドによって識別される。発行人B I A デバイスは正当な装置のデータベースにおいて2（発行人）に設定された使用フィールドによって識別される。

各発行人のターミナルは、それを使うことが承認された10の個人を持ち、各個人デバイスが、2つの追加の承認された個人を持ち、サーバ内には1, 000, 000の個人デバイスがあるとする、A I Dの蓄積は：

$10 \times 100, 000 + 2 \times 1, 000, 000 - 3, 000, 000$ エントリ

を記憶する。データベース全体は約24MBの記憶領域を必要とする。

承認されたオーナーデータベースレコードまたは正当な装置データベースレコードが削除される時、それらを参照している全ての承認された個人レコードが削除される。

以前の詐欺のデータベース

以前の詐欺のデータベース（P F D）は、過去におけるある時点でだまされたメンバー発行人を持つ個人を表わすレコードの集大成である。P F Dはまた、P F D内に一致した記録を持つI B D内の個人を除去するため、低いシステム動作期間の間、背景のトランザクションを走らせる。

個人が再度登録を試みていることを検出しない限り、システムは、自動的に個人をP F D内に入れることはない。個人をP F Dに置くことは、本明細書の範囲外の微妙な施策事項である。

新しいI B Dレコードがアクティブであるとしてマークされる前に、個人の1次的そして2次的なバイオメトリックスは、個人の識別手続きで使用されるものと同じバイオメトリック比較技術を用いてP F Dにおける各々のそして全てのバイオメトリックに対してチェックされる。新しいI B Dレコードに一致が見つかり、I B Dレコードのステータスは「以前の詐欺」に設定される。以前の詐欺のチェックが、登録要求の一部として実行される場合は、G Mは「以前の詐欺を持つ個人を登録中」という警告を出す。

P F Dは、比較的小さいままであると仮定する。自発的でないバイオメトリックサーチのため、P F Dを動かすコストは、高い。

以前の詐欺レコードの概要は：

以前の詐欺：

```
primaryBiometric=Biometric
secondaryBiometric=Biometric
BiometricId=int 4
P I C =char 1 0
phoneNumber=char 1 2
```

```
lastName=char 2 4
firstName=char 2 4
middleInitial=char 2
S S N=char 9
privateSignal=char 4 0
address=char 5 0
ZipCode=char 9
publicKey=char 6 4
checksums=int 4 [1 0]
acctLinks=char 3 0 [1 0]
emergencyIndex=char 1
emergencyLink=char 1
privs=char 1 0
enroller=int 8
emergencyUseCount=int 4
status=int 1
```

ステータス領域は次の1つ：

- 0：停止
- 1：動作（アクティブ）
- 2：以前の詐欺

P F Dは、バイオメトリック識別コードによって鍵をかけられる。

PFDレコードは、IBDレコードと同じである。幸運にも、DPCは、これらのほんの僅かしか記憶する必要がないため、データベース全体を記憶するためには2つのデータベース装置が必要なだけである。これらの内、1つはバックアップである。PFDは、他のいずれのDPC構成要素にも直接依存しない。

RPT→BIA レジスタを割り当てよ 〈1〉 〈1 2 3 4 5 6〉

BIA→RPT OK

RPT→メッセージを形成〈トランザクション〉

BIA→RPT 〈トランザクションリクエストメッセージ〉

BIA→RPT OK

BIA/LCD: 〈DPC本部と対話中〉

RPT→DPC 〈トランザクションリクエストメッセージ〉

DPC: バイオメトリックの有効性証明、アカウント番号取り出し

→4024-2256-5521-1212

DPC→VISA 〈承認 4024-2256-5521-1212
452. 33 123456〉

VISA→DPC 〈OK 4024-2256-5521-1212
452. 33 123456 承認コード〉

DPC: 秘密コード取得

DPC→RPT 〈トランザクションレスポンスメッセージ〉

RPT→BIA レスポンスを示せ〈トランザクションレスポンスメッ
セージ〉 〈8〉

BIA/LCD: 〈トランザクション OK: I am fully persuaded of it〉

BIA→RPT 〈OK 〈承認コード〉〉

RPT: 承認コードをレシートに印刷せよ
インターネットPOS端末 (Internet Point of Sale Terminal)

この場合、IPTはトランザクションの承認のため標準BIA、DPCと通信する。トランザクション量は452. 33、個人アカウントは4024-225

6-5521-1212、インターネット商人はmerchant.comに位置し、その商人コードは123456、そして個人の秘密コードは「I am fully persuaded of it.」である。

IPT→merchant.com 〈リソースが使用可能であれば商人

人コードを私に送れ〉

merchant.com→IPT 〈OK 123456 merchant.com公開鍵〉

IPTはセッション鍵を生成し、merchant.com公開鍵で暗号化

IPT→merchant.com 〈セッション鍵〉

商人との全てのその後の通信はセッション鍵で暗号化

merchant.com→IPT 〈価格及び製品情報〉

IPT／スクリーン：価格及び製品情報を表示

個人：「フルーツケーキ、価格45.33」の項目を選択

IPT→BIA 言語を設定せよ 〈英語〉

BIA→IPT OK

IPT←BIA バイオメトリックを取得せよ 〈20〉

BIA／LCD：〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

BIA→IPT OK

IPT→BIA PINを取得せよ 〈40〉

BIA／LCD：〈あなたのPICを入力し、その後〈入力〉を押して下さい。〉

個人はPICを入力し、その後〈入力〉を押す。

BIA→IPT OK

IPT→BIA アカウント番号を取得せよ 〈40〉

BIA／LCD：〈今度はあなたのアカウントインデックスコードを入力し、その後〈入力〉を押して下さい。〉

個人はコードを入力し、その後〈入力〉を押す。

B I A → I P T O K

I P T → B I A 量の有効性を証明せよ 〈4 5 . 3 3 〉 〈4 0

>

B I A / L C D : 〈量 4 5 . 3 3 O K ?〉

個人はO Kを入力する

B I A → I P T O K

I P T → B I A レジスタを割り当てよ 〈1〉 〈1 2 3 4 5 6〉

B I A → I P T O K

I P T → B I A レジスタを割り当てよ 〈2〉 〈m e r c h a n t .
c o m〉

B I A → I P T O K

I P T → B I A レジスタを割り当てよ 〈3〉 〈フルーツケーキ〉

B I A → I P T O K

I P T → B I A メッセージ形成 〈遠隔トランザクション〉

B I A → I P T 〈遠隔トランザクションリクエストメッセージ〉

B I A → I P T O K

B I A / L C D : 〈D P C 本部と対話中〉

I P T → m e r c h a n t . c o m 〈遠隔トランザクションリクエスト
メッセージ〉

m e r c h a n t . c o m → D P C 公開鍵を用いてD P C と安全接続

m e r c h a n t . c o m → D P C 〈遠隔トランザクションリクエスト
メッセージ〉

D P C : バイオメトリックの有効性証明、アカウント番号取り出し
→ 4 0 2 4 - 2 2 5 6 - 5 5 2 1 - 1 2 1 2

D P C : コード 1 2 3 4 5 6 によりインターネット m e r c h a n
t . c o m の有効性証明

D P C → V I S A 〈承認 4 0 2 4 - 2 2 5 6 - 5 5 2 1 - 1 2 1 2

4 5 . 3 3 1 2 3 4 5 6 >

V I S A → D P C < O K 4 0 2 4 - 2 2 5 6 - 5 5 2 1 - 1 2 1

2 4 5 . 3 3 1 2 3 4 5 6 承認コード>

D P C : 秘密コードを取得

D P C → m e r c h a n t . c o m < トランザクションレスポンスメッセージ>

m e r c h a n t . c o m は承認コードを格納

m e r c h a n t . c o m → I P T < トランザクションレスポンスメッセージ>

I P T → B I A レスポンスを示せ < トランザクションレスポンスメッセージ> < 8 >

B I A / L C D : < トランザクション O K : I am fully persuaded of it >

B I A → I P T < トランザクション O K >

インターネット料金計算ターミナル (Internet Teller Terminal)

この場合、I T T は定型または非定型のホームバンキング操作を実行するために標準 B I A、D P C 及び銀行のインターネットサーバと通信する。D P C は実際には、トランザクションの有効性を承認することには関わらず、ネットワーククレデンシャルの有効セットを作成すること及び銀行との通信回線の確保をすることについてのみ責任を負う。

I T T → b a n k . c o m < リソースが使用可能であれば銀行コードを私に送れ > >

b a n k . c o m → I T T < O K 1 2 0 0 >

I T T → B I A 言語を設定せよ < 英語 >

B I A → I T T O K

I T T → B I A バイオメトリックを取得せよ < 2 0 >

B I A / L C D : < 指を光っているパネルの上に置いて下さい。 >

個人は指をスキャナーの上に置く。

B I A → I T T O K

I T T → B I A P I N を取得せよ 〈40〉

B I A / L C D : 〈あなたの P I C を入力し、その後 〈入力〉 を押して下さい。〉

個人は P I C を入力し、その後 〈入力〉 を押す。

B I A → I T T O K

R P T → B I A アカунツ番号を取得せよ 〈40〉

B I A / L C D : 〈次にアカウントインデックスコードを入力し、そして、〈入力〉を押して下さい〉

個人はコードを入力し、〈入力〉を押す。

B I A → I T T O K

I T T → B I A レジスタを割り当てよ 〈1〉 〈1200〉 (銀行コード)

B I A → I T T O K

I T T → B I A レジスタを割り当てよ 〈2〉 〈bank. com〉

B I A → I T T O K

I T T → B I A レジスタを割り当てよ 〈3〉 〈ITT. port, bank. com. port〉 (TCP / IP アドレス)

B I A → I T T O K

I T T → メッセージを形成せよ 〈ネットクレデンシャル〉

B I A → I T T 〈ネットワーククレデンシャルリクエスト〉

B I A → I T T O K

B I A / L C D : 〈D P C 本部と対話中〉

I T T → D P C 〈ネットワーククレデンシャルリクエスト〉

D P C : バイオメトリックの有効性証明、クレデンシャル (時間、アカウント、銀行) を生成

D P C : 秘密コード取得

D P C → I T T 〈ネットワーククレデンシャルレスポンス〉

I T T → B I A レスポンスを示せ 〈ネットワーククレデンシャルレスポンス〉

B I A はレスポンスを復号化し、レスポンスを検査する

B I A / L C D : 〈クレデンシャル O K : I am fully persuaded of it〉

B I A は銀行の公開鍵を用いて、クレデンシャル、セッション鍵、

チャレンジ鍵を暗号化する

B I A → I T T 〈安全接続リクエストメッセージ〉

B I A → I T T 〈セッション鍵〉

B I A → I T T O K

B I A / L C D : 〈bank. com との安全接続中〉

I T T → bank. com 〈安全接続リクエストメッセージ〉

bank. com は秘密鍵を用いて暗号し、クレデンシャルの有効性を証明し、共用鍵を使用する。

bank. com → I T T 〈O K〉

I T T → bank. com 接続の更なるトランザクションは全て I T T / 銀行セッション鍵を用いて I T T によって暗号化される。

銀行が非定型であると決定するあらゆるトランザクションは、B I A のチャレンジレスポンス機構を用いて個人によって確認されなければならない。チャレンジレスポンス機構は、B I A が「安全接続」状態にある場合にのみ利用可能である。

bank. com → I T T 〈〈有効性証明要求〉の有効性を証明〉

I T T → B I A 秘密 〈暗号化有効性証明要求〉の有効性を証明

B I A はチャレンジセクションを復号化し、表示する。

B I A / L C D : 〈O K です : 1 2 , 4 2 0 . 0 0 から 1 0 2 3 - 3 3 0 2 - 2 1 0 1 - 1 1 0 0 に転送〉

個人は O K を入力する。

B I Aはチャレンジ鍵を用いてレスポンスの再暗号化をする。

B I A／L C D：〈b a n k． c o mに安全接続中〉

B I A→I T T 〈O K 〈暗号化された有効性証明レスポンス〉〉

I T T→b a n k． c o m 〈暗号化された有効性証明レスポンス〉

電子署名端末 (Electronic Signature Terminal)

この場合、E S Tはデジタル署名を作成するため、標準B I A及びD P Cと通信する。個人の秘密コードは「I am fully persuaded of it.」であり、署名される文書は「The Letter of Marque.」と呼ばれる。

C E T→B I A 言語を設定せよ 〈英語〉

B I A→C E T O K

C E T→B I A バイオメトリックを取得せよ 〈20〉

B I A／L C D：〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

B I A→C E T O K

C E T→B I A P I Nを取得せよ 〈40〉

B I A／L C D：〈あなたのP I Cを入力し、その後〈入力〉を押して下さい。〉

個人はP I Cを入力し、その後〈入力〉を押す。

B I A→C E T O K

C E T→B I A 文書の有効性を証明せよ 〈Letter of Marque〉 〈40〉

B I A／L C D：〈文書「Letter of Marque」 O K ?〉

個人はO Kを入力する。

B I A→C E T O K

C E T→B I A レジスタを割り当てよ 〈1〉 〈文書MD 5 値〉

B I A→C E T O K

C E T→メッセージを形成せよ 〈署名提出〉

B I A→C E T 〈電子署名リクエスト〉

B I A → C E T O K

B I A / L C D : < D P C 本部と対話中 >

C E T → D P C < 電子署名リクエスト >

D P C : バイオメトリックの有効性を証明、署名を生成、署名テキストコードを返す

D P C : 秘密コード取得

D P C ← C E T < 電子署名レスポンス >

C E T → B I A レスポンスを示せ < 電子署名レスポンス > < 8 >

B I A / L C D : < 文書 O K : I am fully persuaded of it. >

B I A → C E T < O K < 署名テキストコード > >

認可された電子メールターミナル (Certified Email Terminal)

この場合は、C E T は認可された電子メールを送信するために、標準 B I A 及び D P C と通信する。個人の秘密コードは「I am fully persuaded of it.」であり、文書名は「Post Captain.」である。

C E T → B I A 言語を設定せよ < 英語 >

B I A → C E T O K

C E T → B I A バイオメトリックを取得せよ < 2 0 >

B I A / L C D : < 指を光っているパネルの上に置いて下さい。 >

個人は指をスキャナーの上に置く。

B I A → C E T O K

C E T → B I A P I N を取得せよ < 4 0 >

B I A / L C D : < あなたの P I C を入力し、その後 < 入力 > を押して下さい。 >

個人は P I C を入力し、その後 < 入力 > を押す。

B I A → C E T O K

C E T → B I A 文書の有効性を証明せよ < Post Captain > < 4 0 >

B I A / L C D : < 文書「Post Captain」で O K ? >

個人は O K を入力する。

C E T／スクリーン： 〈受け手リスト？〉

個人は 〈fred@telerate.com joe@reuters.com〉 を入力する。

C E T→B I A レジスタを割り当てよ 〈1〉 〈fred@telerate.com
joe@reuters.com〉

B I A→C E T O K

C E T→メッセージを形成せよ 〈文書提出〉

B I A→C E T 〈電子文書提出リクエスト〉

B I A→C E T O K

B I A／L C D： 〈D P C 本部と対話中〉

C E T→D P C 〈電子文書提出リクエスト〉

D P C：バイオメトリックの有効性を証明、メッセージを生成、メ
ッセージ#001234を返す。

D P C：秘密コード取得

D P C→C E T 〈電子文書提出レスポンス〉

C E T→B I A レスポンスを示せ 〈電子文書提出レスポンス〉 〈8
〉

B I A／L C D： 〈文書O K：I am fully persuaded of it.〉

B I A→C E T 〈文書O K 〈1234〉〉

C E T→D P C 〈電子文書データリクエスト、1234、セクション
1、未完〉

D P C→C E T 〈電子文書データレスポンス、未完〉

C E T→D P C 〈電子文書データリクエスト、1234、セクション
2、未完〉

D P C→C E T 〈電子文書データレスポンス、未完〉

C E T→D P C 〈電子文書データリクエスト、1234、セクション
3、未完〉

D P C→C E T 〈電子文書データレスポンス、未完〉

C E T→D P C 〈電子文書データリクエスト、1234、セクション

4、終了>

D P C → C E T <電子文書データレスポンス、トラック1 2 3 4. 1
1 2 3 4. 2>

D P C → fred@telerate.com <e メール 1 2 3 4. 1 メッセージ
到着>

D P C → joe@reuters.com <e メール 1 2 3 4. 2 メッセージ到
着>

mailer@telerate.com → D P C <1 2 3 4. 1 の受理通知 e メール
>

D P C → sender@company.com <e メール 1 2 3 4. 1 受け手に通
知された>

mailer@reuters.com → D P C <1 2 3 4. 2 の受理通知 e メール
>

D P C → sender@company.com <e メール 1 2 3 4. 2 受け手に通
知された>

[フレッドの C E T では、フレッドは「メッセージ到着」の電子メ
ールメッセージを見て、すぐにそのメッセージを採用することを決
める]

C E T → B I A 言語を設定せよ <英語>

B I A → C E T O K

C E T → B I A バイオメトリックを取得せよ <20>

B I A / L C D : <指を光っているパネルの上に置いて下さい。>

個人は指をスキャナーの上に置く。

B I A → C E T O K

C E T → B I A P I N を取得せよ <40> B I A / L C D : <あな
たの P I C を入力して下さい。>

個人は P I C を入力し、その後 <入力> を押す。

B I A → C E T O K

C E T → B I A レジスタを割り当てよ 〈1〉 〈1 2 3 4. 1〉

B I A → C E T O K

C E T → メッセージを形成せよ 〈文書取り出し〉

B I A → C E T 〈電子文書取り出しリクエスト〉

B I A → C E T O K

B I A / L C D : 〈D P C 本部と対話中〉

C E T → D P C 〈電子文書取り出しリクエスト〉

D P C : バイオメトリックの有効性証明、1 2 3 4. 1 の検索

D P C : 秘密コード取得

D P C → C E T 〈電子文書取り出しレスポンス〉

C E T → B I A レスポンスを示せ 〈電子文書取り出しレスポンス〉
〈8〉

B I A / L C D : 〈文書O K : I am fully persuaded of it.〉

B I A → C E T 〈文書O K 〈メッセージ鍵〉〉

C E T / スクリーン : 復号化し、その後文書表示

安全ファックス端末 (Secure Fax Terminal)

この場合、S F T は安全なファックスを送信するため、B I A / c a t v 及び
D P C と通信する。

S F T → B I A バイオメトリックを取得せよ 〈2 0〉

B I A / L C D : 〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

B I A → S F T O K

B I A / L C D : 〈あなたのP I Cを入力し、その後〈入力〉を押
して下さい。〉

個人はP I Cを入力し、その後〈入力〉を押す。

S F T → B I A P I Nを設定せよ 〈4 0〉

B I A / L C D : 〈あなたのタイトルインデックスを入力し、その
後〈入力〉を押して下さい。〉

個人はタイトルインデックスを入力し、その後〈入力〉を押す。

S F T→B I A タイトルインデックスコードを設定せよ 〈4 0〉

B I A→S F T O K

S F T／スクリーン： 〈受け手？（内線は＊を追加して、最後に
＃を付ける）〉

個人は〈1 5 1 0 9 4 4－6 3 0 0＊5 2 5＃〉を入力

S F T／スクリーン： 〈受け手？（内線は＊を追加して、最後に
＃を付ける）〉

個人は〈1 4 1 5－8 7 7－7 7 7 0＃〉を入力

S F T／スクリーン： 〈受け手？（内線は＊を追加して、最後に
＃を付ける）〉

個人は〈＃〉を入力

S F T→B I A レジスタを割り当てよ 〈1〉 〈1 5 1 0 9 4 4 6 3
0 0＊5 2 5 1 4 1 5 8 7 7 7 7 7 0〉

B I A→S F T O K

S F T－メッセージを形成せよ 〈文書提出〉

B I A→S F T 〈安全ファックス提出リクエスト〉

B I A→S F T O K

B I A／L C D： 〈D P C本部と対話中〉

S F T→D P C 〈安全ファックス提出リクエスト〉

D P C：バイオメトリックの有効性証明、メッセージを生成、メッ
セージ＃0 0 1 2 3 4を返す。

D P C：秘密コード取得

D P C→S F T 〈安全ファックス提出レスポンス〉

S F T→B I A レスポンスを示せ 〈安全ファックス提出レスポンス〉
〈1 0〉

B I A／L C D： 〈文書O K：I am fully persuaded of it.〉

B I A→S F T 〈文書O K 〈0 0 1 2 3 4〉〉

S F T → D P C 〈安全ファックスデータリクエスト、1 2 3 4、セクション 1、未完〉

D P C → S F T 〈安全ファックスデータレスポンス、未完〉

S F T → D P C 〈安全ファックスデータリクエスト、1 2 3 4、セクション 2、未完〉

D P C → S F T 〈安全ファックスデータレスポンス、未完〉

S F T → D P C 〈安全ファックスデータリクエスト、1 2 3 4、セクション 3、未完〉

D P C → S F T 〈安全ファックスデータレスポンス、未完〉

S F T → D P C 〈安全ファックスデータリクエスト、1 2 3 4、セクション 4、終了〉

D P C → S F T 〈安全ファックスデータレスポンス〉

D P C → ファックス接続 1 5 1 0 9 4 4 6 3 0 0

e D P C → S F T 6 3 0 0 〈ファックスの表紙 「Sam Spade」 「Fred Jones」より 1 2 3 4. 1 4 ページ待ち〉

D P C → 接続切断

D P C → ファックス接続 1 4 1 5 8 7 7 7 7 0

e D P C → S F T 7 7 0 0 〈ファックスの表紙 「John Jett」 「Fred Jones」より 1 2 3 4. 2 4 ページ待ち〉

D P C → 接続切断

[サムの S F T では、サムはフレッドから到着した文書ファックスの表紙を見て、トラッキングコード 1 2 3 4. 1 を用いて D P C からの文書の取り出しを開始する。]

S F T → B I A バイオメトリックを取得せよ 〈2 0〉

B I A / L C D : 〈指を光っているパネルの上に置いて下さい。〉

個人(サム)は指をスキャナーの上に置く。

B I A → S F T O K

S F T → B I A P I N を取得せよ 〈4 0〉

B I A / L C D : <あなたの P I C を入力し、その後 <入力> を押して下さい。>

個人は P I C を入力し、その後 <入力> を押す。

B I A → S F T O K

S F T → B I A レジスタを割り当てよ <1> <1 2 3 4. 1>

B I A → S F T O K

S F T → メッセージを形成せよ <文書取り出し>

B I A → S F T <安全ファックス取り出しリクエスト>

B I A → S F T O K

B I A / L C D : <D P C 本部と対話中>

S F T → D P C <安全ファックス取り出しリクエスト>

D P C : バイオメトリックの有効性を証明、1 2 3 4. 1 の検索、
バイオメトリック P I C - Sam Spade を確認する。

D P C : データベースの秘密コードを検索

D P C → S F T <安全ファックス取り出しレスポンス>

S F T → B I A レスポンスを示せ <安全ファックス取り出しレスポ
ンス> <8>

B I A → S F T <文書 O K : I am fully persuaded of it <メッセ
ージ鍵>>

S F T / スクリーン : <文書 O K : I am fully persuaded of it>

S F T / スクリーン : ファックス印字

バイオメトリック登録端末 (Biometric Registration Terminal)

この場合には、B R T は個人をシステムに登録するために、登録 B I A および
D P C と交信する。

B R T → B I A 言語を設定せよ <英語>

B I A → B R T O K

B R T → B I A バイオメトリックを取得せよ <2 0> <人差し指>

B I A / L C D : <人差し指を光っているパネルの上に置いて下さ

い。〉

個人は人差し指をスキャナーの上に置く。

B I A → B R T O K

B R T → B I A バイオメトリックを取得せよ 〈20〉 〈中指〉

B I A / L C D : 〈中指を光っているパネルの上に置いて下さい。

〉

個人は中指をスキャナーの上に置く。

B I A → B R T O K

B R T → B I A P I N を取得せよ 〈40〉

B I A / L C D : 〈あなたの P I C を入力し、その後 〈入力〉 を押して下さい。〉

個人は123456と入力し、その後 〈入力〉 を押す。

B I A → B R T O K

B R T → B I A メッセージ鍵を取得せよ

B I A → B R T 〈O K 〈メッセージ鍵〉〉

B I A → 〈登録要求メッセージ〉

B R T / スクリーン : 〈名前 : 〉

代表者は入力する。〈フレッド = G = シュルツ (Fred G. Shultz)

〉

B R T / スクリーン : 〈住所 : 〉

代表者は入力する。〈メイン州 北 1234〉

B R T / スクリーン : 〈郵便番号〉

代表者は入力する。〈94042〉

B R T / スクリーン : 〈秘密コード〉

代表者は個人に照会し、その後入力する。〈私はそれを完全に信じる。(I am fully persuaded of it.)〉

B R T / スクリーン : 〈資産アカウントリスト〉

代表者は入力する。〈2, 1001-2001-1020-201

1>

(クレジットカード)

代表者は入力する。〈3, 1001-1002-0039-221

2>

(当座預金)

BRT/スクリーン: 〈緊急のアカウント〉

代表者は入力する。〈1, 1001-1002-0039-221

2>

(緊急、当座預金)

BRT→メッセージを作成せよ 〈登録〉

BIA→BRT 〈登録要求メッセージ〉

BIA→BRT OK

BIA/LCD: 〈私はDPC中央と対話している〉

BRTはメッセージ鍵により暗号化された個人情報を要求に付加する。

BRT→DPC 〈登録要求メッセージ〉 〈暗号化された個人情報〉

DPC: PIC123456を検証する。

DPC→BRT 〈登録応答メッセージ〉

BRT→BIA 応答を示せ 〈登録応答メッセージ〉 〈8〉

BIA/LCD: 〈登録OK: 私はそれを完全に信じる。(I am fully persuaded of it.)、123456〉

BIA→BRT 〈OK〉

消費者サービス端末 (Customer Service Terminal)

この場合には、CSTは個人の同一性およびクリデンシャルを検証するために、標準BIAおよびDPCと交信する。

CST→BIA 言語を設定せよ 〈英語〉

BIA→CST OK

CST→BIA バイオメトリックを取得せよ 〈20〉

B I A / L C D : <指を光っているパネルの上に置いて下さい。>

個人は指をスキャナーの上に置く。

B I A → C S T O K

C S T → B I A P I N を取得せよ <40>

B I A / L C D : <あなたの P I C を入力し、その後 <入力> を押して下さい。>

個人は P I C を入力し、その後 <入力> を押す。

B I A → C S T O K

C S T → B I A メッセージ鍵を取得せよ

B I A → C S T <O K <メッセージ鍵>>

C S T → メッセージを作成せよ <個人同一性要求>

B I A → C S T <個人同一性要求>

B I A → C S T O K

B I A / L C D : <私は D P C 中央と対話している>

C S T → D P C <個人同一性要求>

D P C : 秘密コード、すなわち個人の秘密コード (priv) を取得する。

D P C → C S T <個人同一性返答>

C S T → B I A 応答を示せ <個人同一性返答> <8>

B I A / L C D : <同一性 O K : 私はそれを完全に信じる。(I am fully persuaded of it.)>

B I A → C S T <O K <個人名秘密コード (priv)>>

C S T : C S T の使用にとって十分であるか知るために秘密コード (priv) を検査する。

発行者端末 (Issuer Terminal)

この場合、I T はアカウントの追加および削除の要求のバッチを承認し、D P C に対して送信するために、標準 B I A および D P C と交信する。個人の秘密コードは「私はそれを完全に信じる。(I am fully persuaded of it.)」であり

、銀行コードは1200である。

I T→B I A 言語を設定せよ〈英語〉

B I A→I T O K

I T→B I A バイオメトリックを取得せよ〈20〉

B I A／L C D：〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

B I A→I T O K

I T→B I A P I Nを取得せよ〈40〉

B I A／L C D：〈あなたのP I Cを入力し、その後〈入力〉を押して下さい。〉

個人はP I Cを入力し、その後〈入力〉を押す。

B I A→I T O K

I T→B I A レジスタを割り当てよ〈1〉〈1200〉

B I A→I T O K

I T→B I A メッセージ鍵を取得せよ

B I A→I T 〈メッセージ鍵〉

B I A→I T O K

I T→B I A メッセージを作成せよ〈発行者要求〉

B I A→I T 〈発行者バッチ要求〉

B I A→I T O K

B I A／L C D：〈私はD P C中央と対話している〉

I T→D P C 〈発行者バッチ要求〉〈メッセージ鍵により暗号化された発行者バッチ〉

D P C：B I Aの識別に対してバイオメトリックの有効性を証明し

、

銀行コードの有効性を証明する。

D P C：秘密コードを取得する。

D P C：メッセージ鍵を用いてメッセージを復号化し、発行者バツ

チを実行する。

D P C → I T 〈発行者バッチ返答〉

I T → B I A 応答を示せ〈発行者バッチ返答〉〈8〉

B I A / L C D : 〈バッチOK : 私はそれを完全に信じる。(I am fully persuaded of it.)〉

B I A → I T 〈OK〉

自動預金支払機 (Automated Teller Machinery)

この場合、A T Mは個人を識別し、銀行アカウント番号を取得するために、統合されたA T M B I AおよびD P Cと交信する。個人のアカウントは2 1 0 0 - 0 2 4 5 - 3 7 7 8 - 1 2 0 1であり、銀行コードは2 1 0 0であり、個人の秘密コードは「私はそれを完全に信じる。(I am fully persuaded of it.)」である。

A T M → B I A バイオメトリックを取得せよ〈20〉

A T M / L C D : 〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

B I A → A T M OK

A T M / L C D : 〈あなたのP I Cを入力し、その後〈入力〉を押して下さい。〉

個人はA T Mのキーボード上で1 2 3 4 5 6を入力し、その後〈入力〉を押す。

A T M → B I A P I Nを設定せよ〈1 2 3 4 5 6〉

B I A → A T M OK

A T M / L C D : 〈それではあなたのアカウント索引コードを入力し、その後〈入力〉を押して下さい。〉

個人は2を入力し、その後〈入力〉を入力する

A T M → B I A アカウント索引コードを設定せよ〈2〉

B I A → A T M OK

A T M - B I A レジスタを割り当てよ〈1〉〈2 1 0 0〉

B I A → A T M O K

A T M → メッセージを作成せよ 〈アカウントアクセス〉

B I A → A T M 〈アカウントアクセス要求メッセージ〉

B I A → A T M O K

A T M / L C D : 〈私はD P C 中央と対話している〉

A T M → D P C 〈アカウントアクセス要求メッセージ〉

D P C : バイオメトリックの有効性を証明し、アカウント番号〉 2
1 0 0 0 2 4 5 3 7 7 8 1 2 0 1 を取り出す。

D P C : 秘密コードを取得する。

D P C → A T M 〈アカウントアクセス応答メッセージ〉

A T M → B I A 応答を復号化せよ 〈アカウントアクセス応答メッセージ〉

B I A → A T M 〈2 1 0 0 - 0 2 4 5 - 3 7 7 8 - 1 2 0 1〉 〈緊急
ではない〉 〈私はそれを完全に信じる。(I am fully persuaded of
it.)〉

A T M / L C D : 〈私はそれを完全に信じる。(I am fully persu-
aded of it.)〉

この時点では、A T M は続ける必要があるアカウント番号を持っているため、
アカウント番号に関連した情報を取り出し、個人との対話を始める。

電話 P O S 端末 (Phone Point of sale Terminal)

この場合、P P T は安全に電話を使って情報をダウンロードし、物品を購入す
るために、統合された電話 B I A および電話マーチャントと交信する。個人の P
I C は 1 2 3 4 であり、アカウント索引コードは 1 であり、マーチャントの電話
番号は 1 8 0 0 5 4 2 - 2 2 3 1 であり、マーチャントコードは 1 2 3 4 5
6 であり、実際のアカウント番号は 4 0 2 4 - 2 2 5 6 - 5 5 2 1 - 1 2 1 2 で
ある。

ここで、電話が電話番号をシステムに渡す前に、電話番号から地域コード (1
- 8 0 0) を取り除くことに注意すること。

個人は電話で18005422231をダイヤルする。

PPT→マーチャント18005422231に接続する

PPT→BIA レジスタを割り当てよ1<5422231>

販売データベース (Sales rep) は答える。個人は物品「フルーツケーキ」を選ぶ。販売データベースは情報をダウンロードする。

マーチャント→PPT <123456 フルーツケーキ 43.54>

PPT→BIA バイオメトリックを取得せよ<20>

電話/LCD: <指を光っているパネルの上に置いて下さい。>

個人は指をスキャナーの上に置く。

BIA→PPT OK

電話/LCD: <あなたのPICを入力し、その後#を押して下さい。>

個人はキーパッド上で1234を入力し、その後#又は* (入力) を入力する。

PPT→BIA PINを設定せよ<1234>

BIA→PPT OK

電話/LCD: <それではあなたのアカウント索引コードを入力して下さい。>

個人は1を入力し、その後<入力>を入力する

RPT→BIA アカウント索引コードを設定せよ<1>

BIA→PPT OK

RPT→BIA レジスタを割り当てよ<2> <123456>

BIA→PPT OK

電話/LCD: <数量45.54でよければ#を押して下さい。>

個人は# (はい) を入力する。

PPT→BIA 数量を設定せよ<43.54>

BIA→PPT OK

P P T→メッセージを作成せよ〈リモートトランザクション〉

B I A→P P T 〈リモートトランザクション要求〉

B I A→P P T O K

電話／L C D：〈私はD P C中央と対話している〉

P P T→マーチャント 〈電話トランザクション要求〉

マーチャント→D P C D P C公開鍵を用いて安全にD P Cに接続する。

マーチャント→D P C 〈電話トランザクション要求〉

D P C：バイオメトリックの有効性を証明し、アカウント番号を取り出す。→4 0 2 4－2 2 5 6－5 5 2 1－1 2 1 2

D P C：マーチャント5 4 2 2 2 3 1がコード1 2 3 4 5 6を有することの有効性を証明する。

D P C→V I S A 〈4 0 2 4－2 2 5 6－5 5 2 1－1 2 1 2 4 3 . 5 4 1 2 3 4 5 6を承認せよ〉

V I S A→D P C 〈O K 承認コード4 0 2 4－2 2 5 6－5 5 2 1－1 2 1 2 4 3 . 5 4 1 2 3 4 5 6〉

D P C：秘密コードを取得する。

D P C→マーチャント 〈トランザクション応答要求〉

マーチャントは応答コードを検査する。

マーチャント→P P T 〈トランザクション応答メッセージ〉

P P T→B I A 応答を復号化せよ〈トランザクション応答メッセージ〉

B I A→P P T 〈O K 〈私はそれを完全に信じる。(I am fully persuaded of it.)〉 〈承認コード〉〉

電話／L C D：〈チャイム〉トランザクションO K：私はそれを完全に信じる。(I am fully persuaded of it.)

ケーブルテレビP O S端末 (Cable-TV Point of sale terminal)

この場合、C P Tは安全にケーブルテレビの広帯域ネットワークを使って情報をダウンロードし、物品を購入するために、統合されたケーブルテレビB I Aお

よび電話マーチャントと交信する。個人のP I Cは1 2 3 4であり、アカウント索引コードは1であり、チャンネルは5であり、マーチャントコードは1 2 3 4 5 6であり、実際のアカウント番号は4 0 2 4-2 2 5 6-5 5 2 1-1 2 1 2である。

個人はテレビのチャンネルを5に合わせる。

マーチャント→C P T 〈フルーツケーキ 4 3. 5 4 1 2 3 4 5 6〉
> (放送)

個人はテレビのリモコン上の「買う」を押す。

C P T／テレビ：〈フルーツケーキを4 3. 5 4ドルで購入中〉

C P T→B I A バイオメトリックを取得せよ〈2 0〉

C P T／テレビ：〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

B I A→C P T O K

C P T／テレビ：〈あなたのP I Cを入力し、その後〈入力〉を押して下さい。〉

個人はキーパッド上で1 2 3 4を入力し、その後「買う」を入力する。

C P T→B I A P I Nを設定せよ〈1 2 3 4〉

B I A→C P T O K

C P T／テレビ：〈それではあなたのアカウント索引コードを入力して下さい。〉

個人は1を入力し、その後〈入力〉を入力する

R P T→B I A アカウント索引コードを設定せよ〈1〉

B I A→C P T O K

R P T→B I A レジスタを割り当てよ〈1〉〈チャンネル5、1 5 :

3 0 : 2 0 P S T〉

B I A→R P T O K

C P T→B I A レジスタを割り当てよ〈2〉〈1 2 3 4 5 6〉

B I A → C P T O K

C P T / テレビ：〈数量 4 5 . 5 4 でよければ「買う」を押して下さい。〉

個人は「買う」を入力する。

C P T - B I A 数量を設定せよ 〈4 3 . 5 4〉

B I A → C P T O K

C P T → メッセージを作成せよ 〈ケーブルテレビトランザクション〉

B I A → C P T 〈ケーブルテレビトランザクション要求〉

B I A → C P T O K

C P T / テレビ：〈私は D P C 中央と対話している〉

C P T → C T V センター 〈ケーブルテレビトランザクション要求〉

C T V センター → マーチャント 〈ケーブルテレビトランザクション要求〉

マーチャント → D P C D P C 公開鍵を用いて安全に D P C に接続する。

マーチャント _ D P C 〈ケーブルテレビトランザクション要求〉

D P C : バイオメトリックの有効性を証明し、アカウント番号を取り出す。→ 4 0 2 4 - 2 2 5 6 - 5 5 2 1 - 1 2 1 2

D P C : チャンネル 5 で現在放映されているマーチャントがコード 1 2 3 4 5 6 を有することの有効性を証明する。

D P C → V I S A 〈4 0 2 4 - 2 2 5 6 - 5 5 2 1 - 1 2 1 2 4 3 . 5 4 1 2 3 4 5 6 を承認せよ〉

V I S A → D P C 〈O K 承認コード 4 0 2 4 - 2 2 5 6 - 5 5 2 1 - 1 2 1 2 4 3 . 5 4 1 2 3 4 5 6〉

D P C : 秘密コード、郵送先住所を取得する。

D P C → マーチャント 〈トランザクション応答要求〉

マーチャントは応答コードを検査し、郵送先住所を記録する。

マーチャント → C T V センター 〈トランザクション応答メッセージ〉

C T Vセンター→C P T <トランザクション応答メッセージ>

C P T→B I A 応答を復号化せよ <トランザクション応答メッセージ>

B I A→C P T <O K <私はそれを完全に信じる。(I am fully persuaded of it.)> <承認コード>>

C P T／テレビ：<チャイム> トランザクションO K：私はそれを完全に信じる。(I am fully persuaded of it.)

前述の内容より、いかにして本発明の目的および特徴が実現されるかが評価されるであろう。

第一に、本発明は使用者がシステムアクセス要求を開始する目的で、トークンのような物理的な物体を所持し、提出する必要をなくすコンピューター識別システムを提供する。第二に、本発明は所有者の物体と情報を所持することを検証する

ることに対向したものとして、使用者の同一性を検証することが可能なコンピューター識別システムを提供する。第三に、本発明は使用者にとって身体的に個人的な1以上の特徴に基づいて、使用者の同一性を検証する。第四に、本発明は承認されていない使用者による不正なアクセスの試みに対して高い抵抗性を有する、コンピューターシステムに安全にアクセスできるシステムを提供する。第五に、本発明は電子メッセージおよび／又はファクシミリの送り手と受け手の識別を可能にする識別システムを提供する。

本発明は特定のトークン不要の識別システムおよび方法に関して述べられているが、本発明から離れることなく装置および方法の様々な変形が可能であることは評価されるであろう。そして本発明は、以下に述べられた請求項により定義される。

用語解説

アカウント索引コード：

特定の金融資産アカウントに対応した単一の数字又は英数字の連続。

A I D：

承認された個人データベース：個人および発行者B I Aの装置を使用

するために承認された個人のリストを含む。

A O D :

装置所有者データベース：各々の B I A についての、地理的および接続の情報を含む中央データベース。

A S C I I :

情報交換のためのアメリカ標準コード。

A T M :

自動預金支払機：金融資産管理システムへのアクセスを行うために符号化されたバイオメトリック同一性情報を使用する。金融資産管理には、現金引き出し管理およびアカウント管理を含む。

B I A :

バイオメトリック入力装置；バイオメトリック同一性情報を集め、それを符号化し暗号化する。またそれを承認できるようにする。異なるハードウェアのモデルおよびソフトウェアのバージョンが入ってくる。

バイオメトリック：

個人の身体的外観のいくつかの側面につきシステムにより行われる測定。

バイオメトリック I D :

個人のバイオメトリック記録を独特に識別するためシステムにより用いられる識別子（I R I D—個人の記録 I D）。

B I O—P I C グループ：

同一の個人識別コードと関連した、アルゴリズム的に非類似のバイオメトリックのサンプル。

B R T :

バイオメトリック登録端末；リテイルバンキングの出口に位置し、バイオメトリック登録情報を個人と結びつける。バイオメトリック登録情報は、選ばれた P I N およびシステムに個人を登録するための選ばれた個人情報である。

C B C :

暗号ブロック連結；D E Sのための暗号化モード。

C C D :

荷電結合素子。

C E T :

保証された電子メール端末；送り手を認識するためにB I Aを使用し、文書を暗号化し、システムに送信する。システムはシステム内のメッセージの到着を維持し、それを受け手に告知する。伝送装置への告知は、文書が送られると行われる。文書は検証されて送信され、B I A暗号化により安全に保たれる。伝送装置は送信状況を調査することもある。参加者は両方ともシステムのメンバーでなければならない。

コマンド：

D P C内で繰り返されるプログラム又はサブルーチンであり、特定のタスクを実行し、B I Aを装備した端末から送られる要求メッセージによって活性化する。

契約受諾／拒否：

個人が自分のB I O－P I Cを入力し、相手方の個人に電子ファクシミリで送信した文書内に含まれる、当該個人の契約の受諾又は拒否の単語を登録させるためにD P Cに命令する過程。

C P T :

ケーブルテレビP O S端末：テレビの上のケーブルボックスに製品の映像とともに製品情報を知らせるデジタル信号を、同時放送するオンスクリーンディスプレイと、バイオメトリックP I N有効化をC A T Vコミュニケーションネットワークを用いて実行するB I A制御リモコンを結合したもの。注文／承認／郵送先住所／物品I Dがマーチャントに送られる。承認の結果はテレビ上に表示される。

C S T :

消費者サービス端末；アカウントの問題から人々を救うために、（アクセス特権に基づいて）アクセスの度合いを検査することで、個人の情報を取り出し、変形することができる能力をシステム消費者サービス職員に与える。

データシーリングステップ：

そのままのテキストを暗号テキストに変換すること（「暗号化」として知られる）。変換は、メッセージの暗号化されたチェックサム生成との組み合わせで行われる。いかなる実質的なメッセージの変形も検出する手段を同時に提供することにより、情報がそのままのテキストに残ることを可能にする。

D E S：

デジタル暗号化標準：暗号によるデジタルデータの保護のための標準。
標準 A N S I X 3. 9 2 - 1 9 8 1 参照。

決定：

処理されて実行ステップ中にあるコマンドの状態。

D P C：

データ処理センター。すなわち、複数ギガバイトのバイオメトリック同一性データベースをサポートする目標のために、ハードウェア、ソフトウェアおよび職員が配置されている場所および要素。D P C は電子メッセージを処理する。そして、ほとんどの電子メッセージは資金の移動、ファックスの送信、又は電子メールの送信のような何らかの行動を実行する準備としてバイオメトリック同一性検査の実行を包含する。

D S P：

デジタル信号プロセッサ：集積回路の一分類であり、信号処理アプリケーションにより要求される数学的操作に特化している。

D U K P T：

トランザクションについて固有の派生した鍵：標準 A N S I / A B A X 9. 2 4 - 1 9 9 2 参照。

E D D :

電子文書データベース：すべての通信中のファックスおよび個人の読み取りを待っている電子メッセージを含む中央データベース。

緊急アカウント索引：

個人により選択される英数字又はその連続であって、アクセスされた時は、システムにより緊急トランザクションとしてラベル付けされたトランザクションとなる。潜在的には誤りスクリーンの表示、および／又は当該個人が伝送又はトランザクションの実行を強制された旨の承認の告知を引き起こす。

E S D :

電子署名データベース：すべてのMD 5 およびすべての文書のいかなる人により署名された電子署名も含む中央データベース。承認番号により参照される。

E S T :

電子署名端末；個人の識別のためにB I Aを使用する。コンピューターは文書のチェックサムを計算し、システムにチェックサムを送る。システムは有効化し、タイムスタンプを付し、チェックサムを保存し、署名コード (sig code) とともに返す。通信手段としてインターネットを使用する。E S Tはまた署名コードおよびMD 5 計算を与えられた署名を検証する。

F A R (誤り受け取り率) :

ある個人のバイオメトリックが誤って他の個人のバイオメトリックとして識別される統計的近似値。

誤りスクリーン：

微妙に不正確になるように意図的に予め決められた情報の表示であり、他人が情報の変化を知らないでいる限り、他人に違法に個人の金融資産についての正確なデータを得させないようにしている。

F D D I :

ファイバーデジタル機器インターフェース：ファイバー光トークンリングを使えるようにするためのネットワーク機器。

F S :

フィールドセパレータ。

F W :

ファイアウォール機器：D P Cに入り、D P Cから出るトラフィックを規制するインターネットルータ。

G M :

ゲートウェイ機器：D P C内の主要処理コンピュータであり、ほとんどのソフトウェアを動作させる。

I B D :

個人バイオメトリックデータベース：バイオメトリック、金融資産、および他の個人情報のための中央データベース。バイオメトリックデータベースに対する調査はトランザクション承認および伝送のために用いられる。

I D :

発行者データベース：金融資産アカウント番号を追加し、削除することを許可する構成を含む中央データベース。

I M L :

I B D機器リスト：どのI B D機器がどのP I Nコードに対応できるかを決定するソフトウェアモジュール。

インターネットマーチャント：

インターネット電子ネットワークの手段によりサービス又は物を消費者に売るリテールアカウント。

I P T :

インターネットP O S端末：インターネットからの品目およびマーチャントコード、有効化のためのB I AバイオメトリックP I Nをインターネットを使ってシステムに送信し、承認／注文／P O #をマーチャン

トに転送する。システムもインターネットを使って応答し、結果をスクリーンに表示する。

発行者：

D P Cで登録される金融資産のための金融アカウント発行者。

発行者バッチ：

D P Cに対する発行者によって検証され、入力されるバイオメトリック I D、金融資産アカウント、アカウント索引コードと共に完成する

「追加」および「削除」命令の集まり。

I T：

発行者端末；特定の個人の I B D記録から（彼ら自身の）金融資産アカウント番号を追加し、削除するために、システムに関連あるバッチを発行者に提供する。

I T T：

インターネット対話端末；バイオメトリック I Dを用いて D P Cから得られる暗号化された証明書を使って、ネットワーク端末セッションを承認する。

L C D：

液晶ディスプレイ：テキストを表示するために用いられる技術。

M A C：

メッセージ承認コード：暗号化チェックサムアルゴリズム。M A Cは M A Cの計算後変更されていないメッセージの内容に保証を与える。A N S I X 9. 9-1986 参照。

M A C M：

メッセージ承認コードモジュール：行きおよび帰りのパケットのための M A Cが行う有効化および生成を扱う D P C内のソフトウェアモジュール。

M D M：

メッセージ復号化モジュール：B I A機器からの、あるいはB I A機

器へ向かうパケットを暗号化し、復号化するD P C内のソフトウェアモジュール。

M P M :

メッセージ処理モジュール：要求パケットの処理を行うD P C内のソフトウェアモジュール。

ネットワーククリデンシャル：

個人と銀行の双方がD P Cによりネットワーククリデンシャルを作るために識別される。証明書は接続の状況（例えば、T C P / I P ソース・ディスティネーションポート）と共に、個人の識別を含む。D P C は個人のアカウント I D、時刻および銀行コードを用いてネットワーククリデンシャルを作る。D P C は公開鍵による暗号化およびD P C の秘密鍵を用いてこのクリデンシャルに署名する。

P F D :

以前の詐欺行為データベース：関連して詐欺行為があったI B D記録のための中央データベース。すべての新しい消費者のバイOMETリックスは、常習犯を減らすために全てのP F D記録に対して検査される。

P G L :

P I N グループリスト：I B C 機器の構成を維持するために責任を有するD P C内のソフトウェアモジュール

P I N :

個人識別番号；少なくとも1つの番号からなる秘密の知識を通じて、個人のアカウントに対するアクセスを防止する方法。

P I C :

個人識別コード；数字、記号又はアルファベット文字から作成されるP I N。

P O S :

ポイント・オブ・セール；物が売られる場所。

P P T :

電話 P O S 端末； B I A を装備した電話を通じてのトランザクションを承認するため、電話番号をマーチャントの価格・製品情報に結合させる。

注文／承認／郵送先住所／ P O はマーチャントに転送される。承認の結果は個人の秘密コードとともに電話の L C D 上に表示され、又は「話される」。

R A M :

ランダムアクセスメモリ。

R F :

無線周波数：一般に電気機器の通常動作中に放出される高周波エネルギーのことをいう。

レジスタ：

特定の目的、データのために予約されるメモリ。集積回路の脇に置かれ、命令に対してオペランドを蓄える。

要求：

B I A から D P C に対しての電子命令であり、 D P C に個人を識別し、その後識別に成功すれば個人のコマンドを処理するように命令する。

R M D :

遠隔マーチャントデータベース：マーチャントの電話と、ケーブルテ

レビ注文店についての、マーチャント I D で索引付けされたすべてのマーチャントの識別コードを含む。マーチャントごとのシステムの暗号化コードも含む。

R P T :

リテール P O S 端末；暗号化されたバイオメトリック同一性情報を、リテールトランザクション情報（現金レジスターからの情報の場合もある）に結合させる。また、システムの承認要求を X. 2 5 ネットワーク、モデム等を使って案出する。

安全伝送：

少なくとも一人の参加者がD P Cに識別されている場合における電子メッセージ又はファクシミリ。

S F T：

安全ファックス端末；送り手を識別するためにB I Aを用いる。安全にされていないファックス、送り手により安全にされているファックス、安全にされているファックス、証明書により安全にされているファックスのいずれも送信する。後者の2つについては、受け手がバイオメトリックP I Nを用いて自分自身を識別することが要求される。行きのファックスをラベル付けするために「タイトル」（タイトル索引数字を用いて特定される）を用いる。送り手は伝達状況を調べることもある。双方の参加者はシステムのメンバーでなければならない。送り手と受け手のいずれもがファックスが実現されることを要求できる。

S N M：

連続番号モジュール：帰りの要求パケットのためのD U K P T連続番号処理を扱うD P C内のソフトウェアモジュール。連続番号処理は再試行（replayattacks）を防止する。

端末：

バイオメトリックサンプルを集め、要求メッセージを形成するためにB I Aを使用する装置。要求メッセージはその後承認および実行のためにD P Cに送信される。端末はほとんど常に、要求メッセージに相手方および同様の者を識別する補助的な情報を付加する。

タイトル索引コード：

個人の承認された役割又は能力を、その個人の職業の状況と共に固有に識別する英数字の連続。

トークン：

能力を与える動かない物体。

トラッキングコード：

D P Cにより蓄積され又は伝送されたデータに割り当てられた英数字の連続。連続は、データを回復（recall）し、データ伝送の状態についての報告を得るために用いられることもあるように、割り当てられている。

トランザクション：

電子による金融の取引。

伝送：

電子による金融の取引以外の電子のメッセージ（message）。

V A D：

有効装置データベース：B I Aの所有者に加えて、各々のB I A（関連する特有の暗号化コードとともに）が認識される、中央データベース。

【図1】

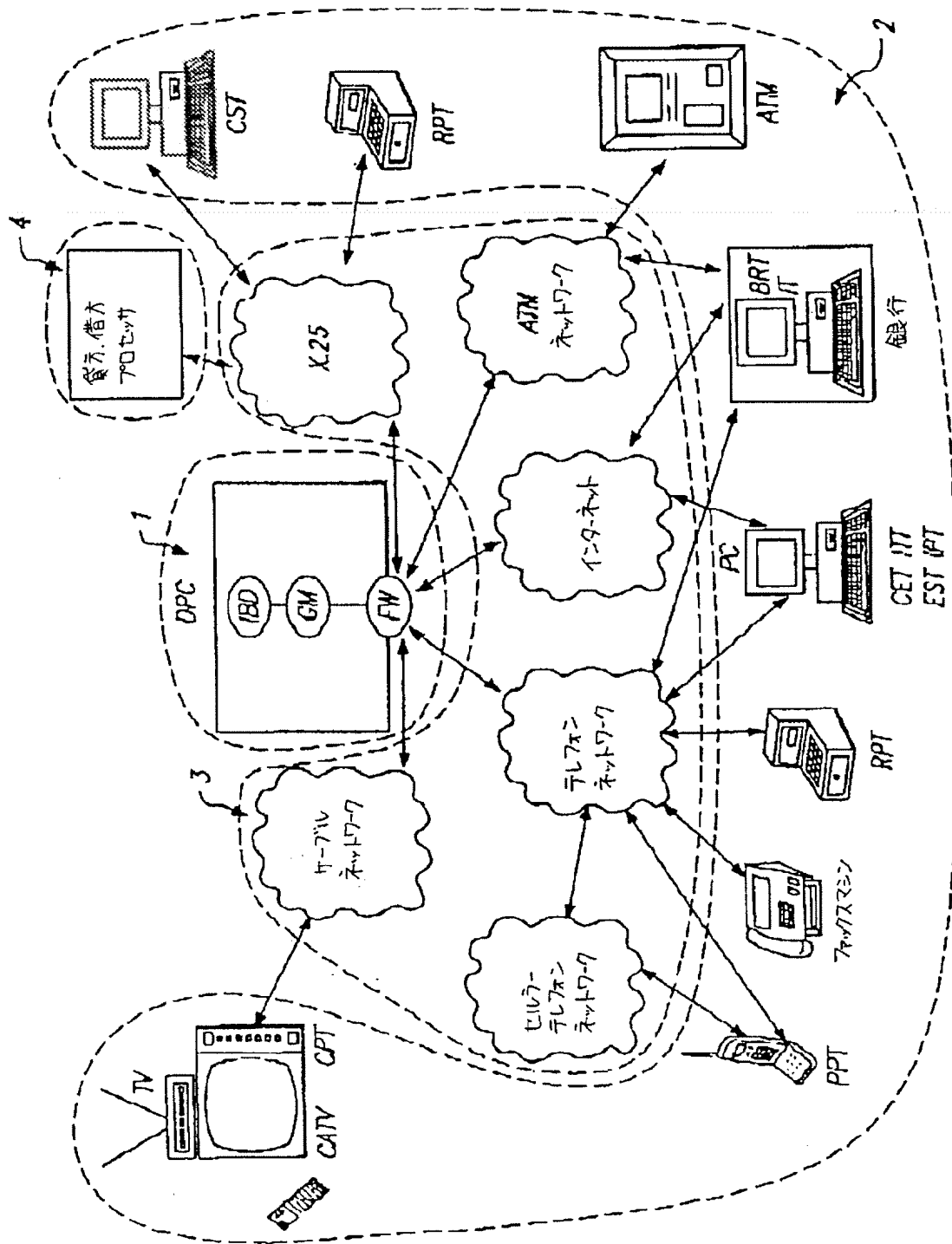


FIG. 1

【図3】

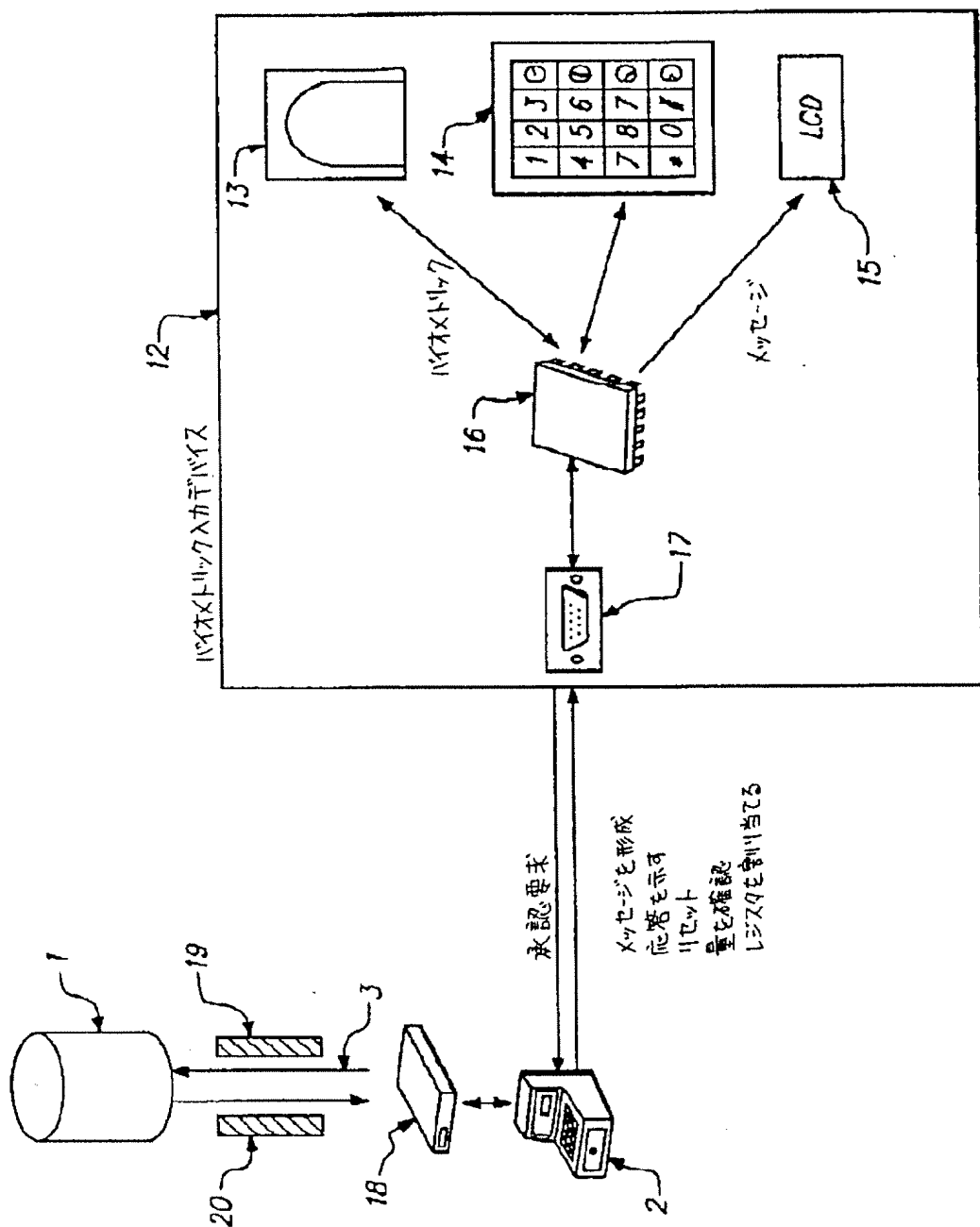


FIG. 3

【図4】

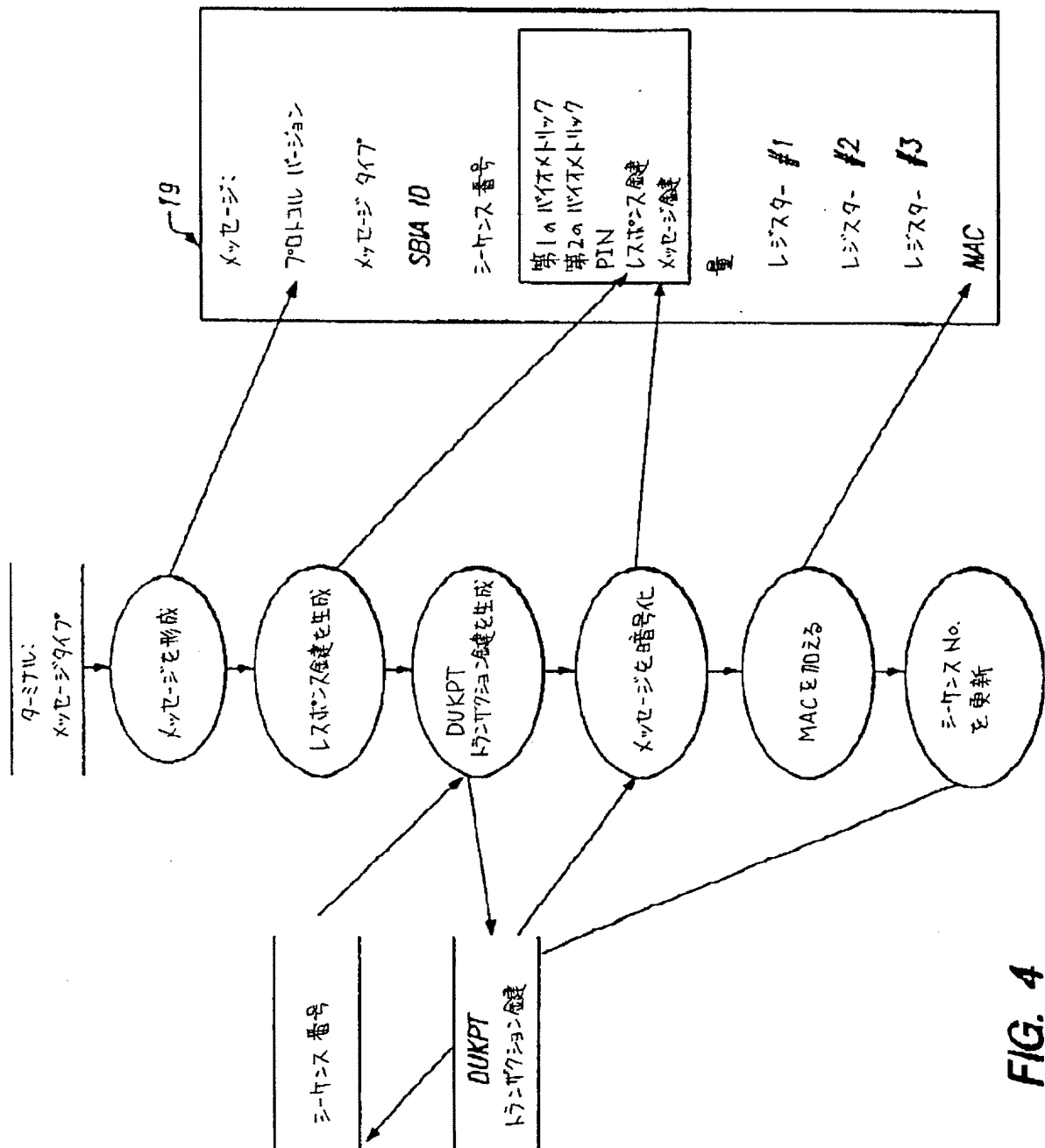


FIG. 4

【図 5】

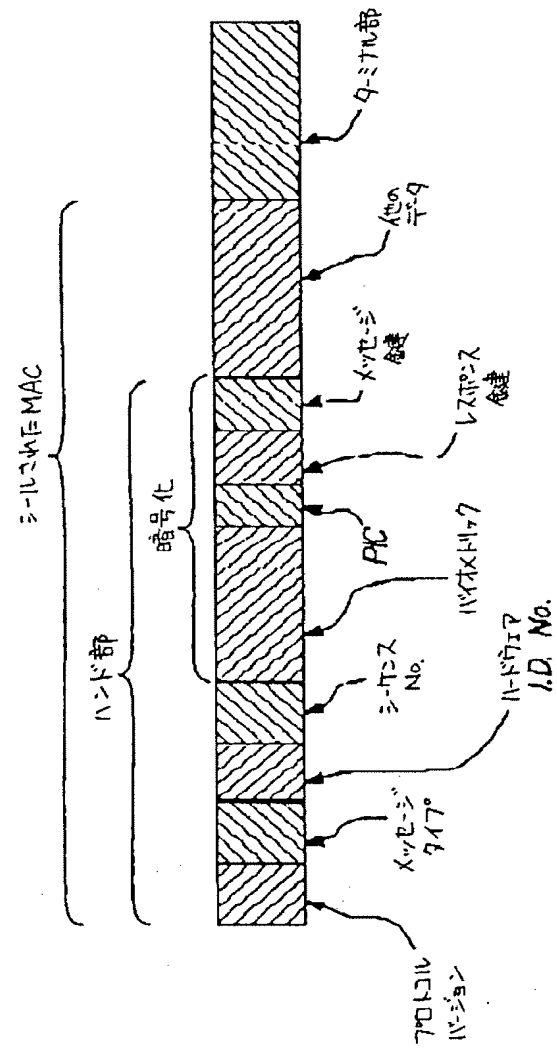


FIG. 5

【図6】

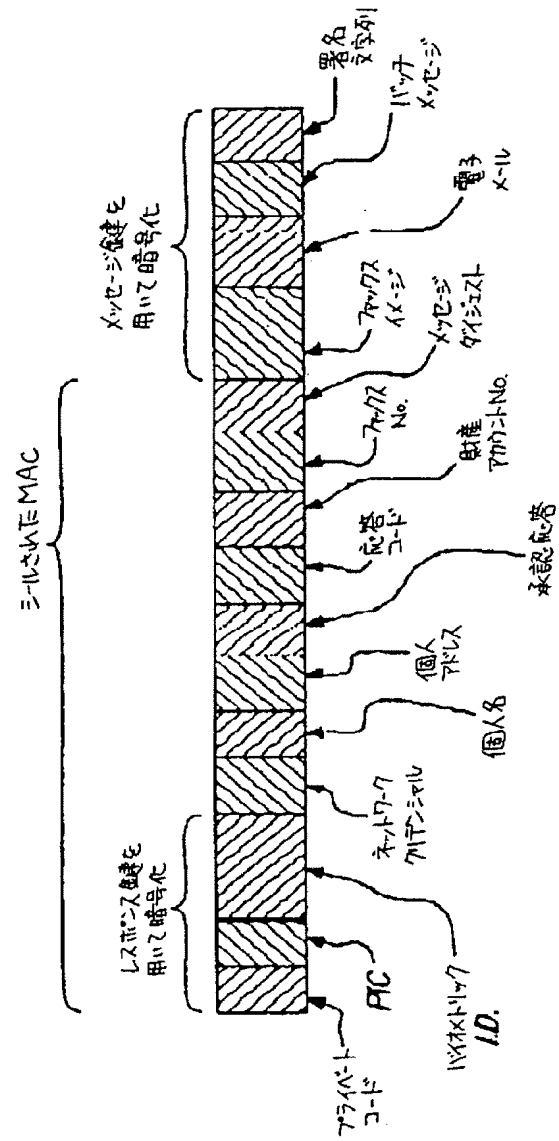


FIG. 6

【図 7】

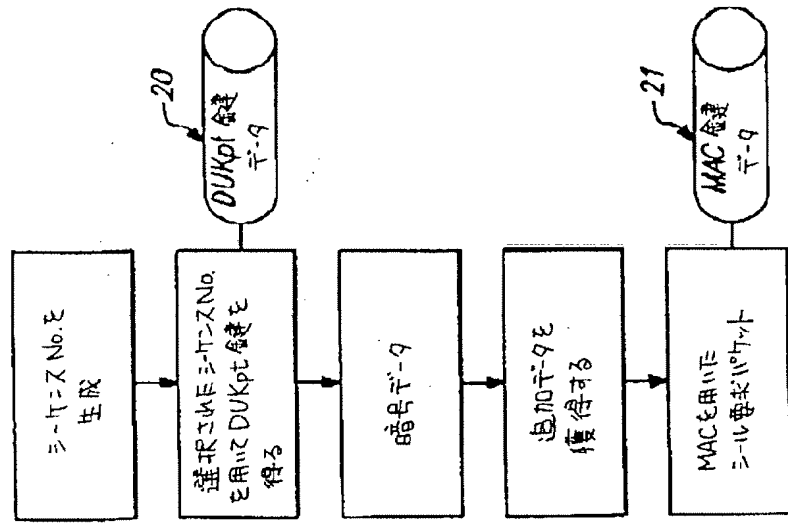


FIG. 7

【図 8】

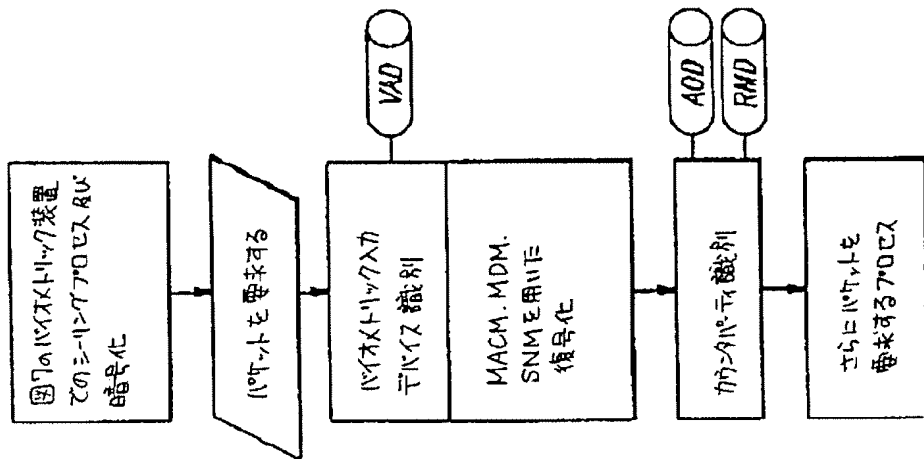


FIG. 8

【図 9】

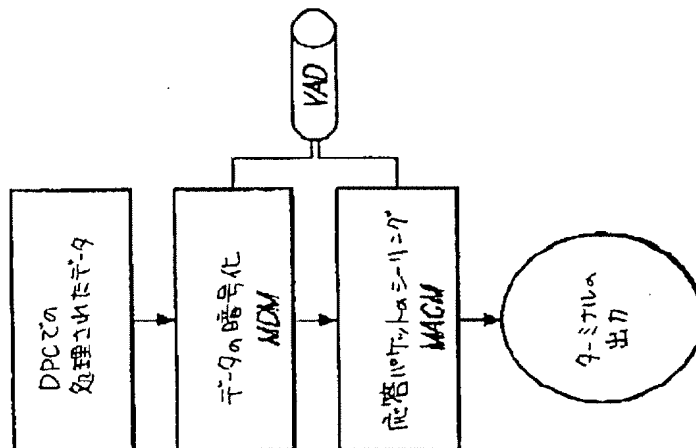


FIG. 9

【図10】

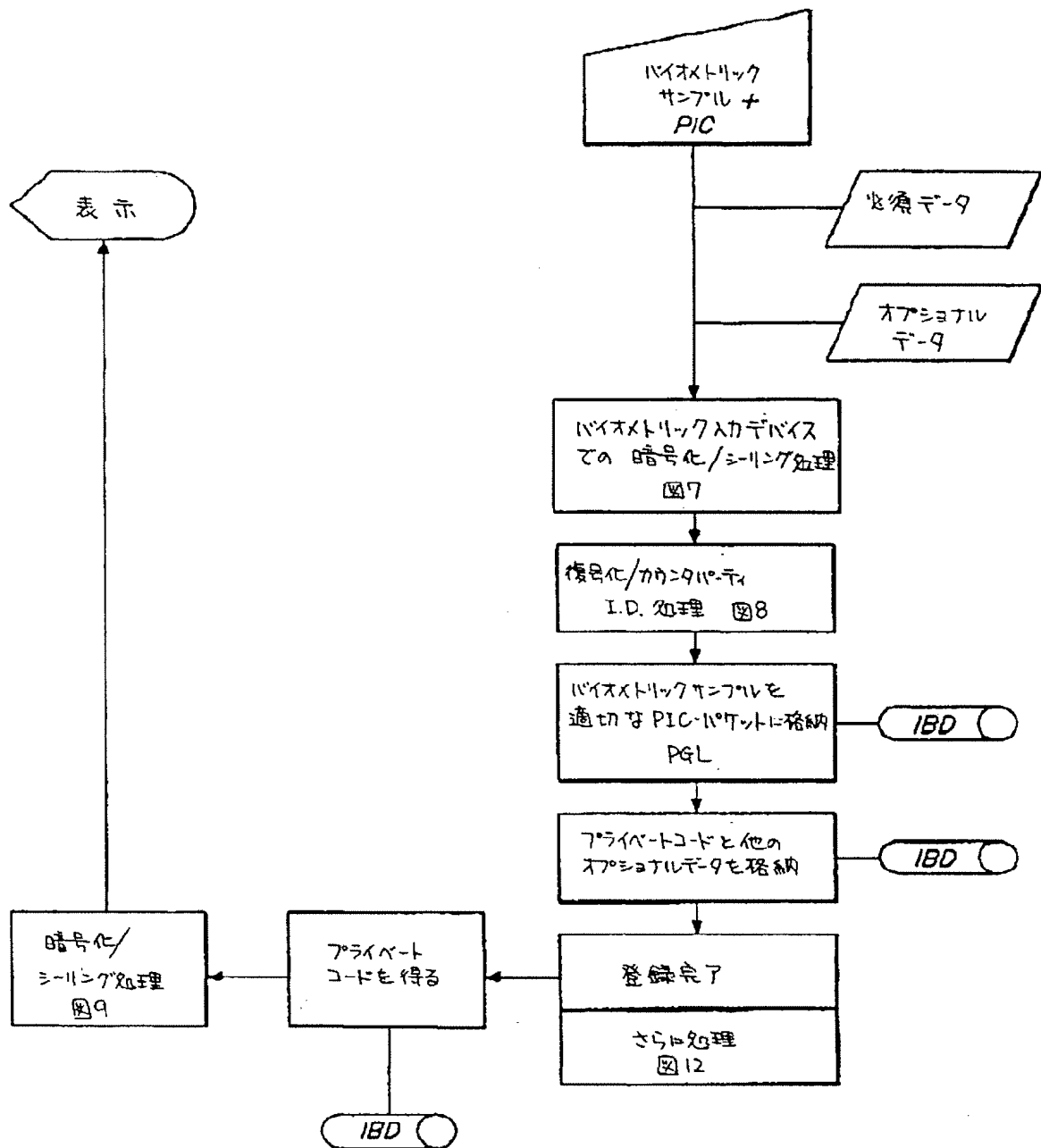


Fig. 10

【図11】

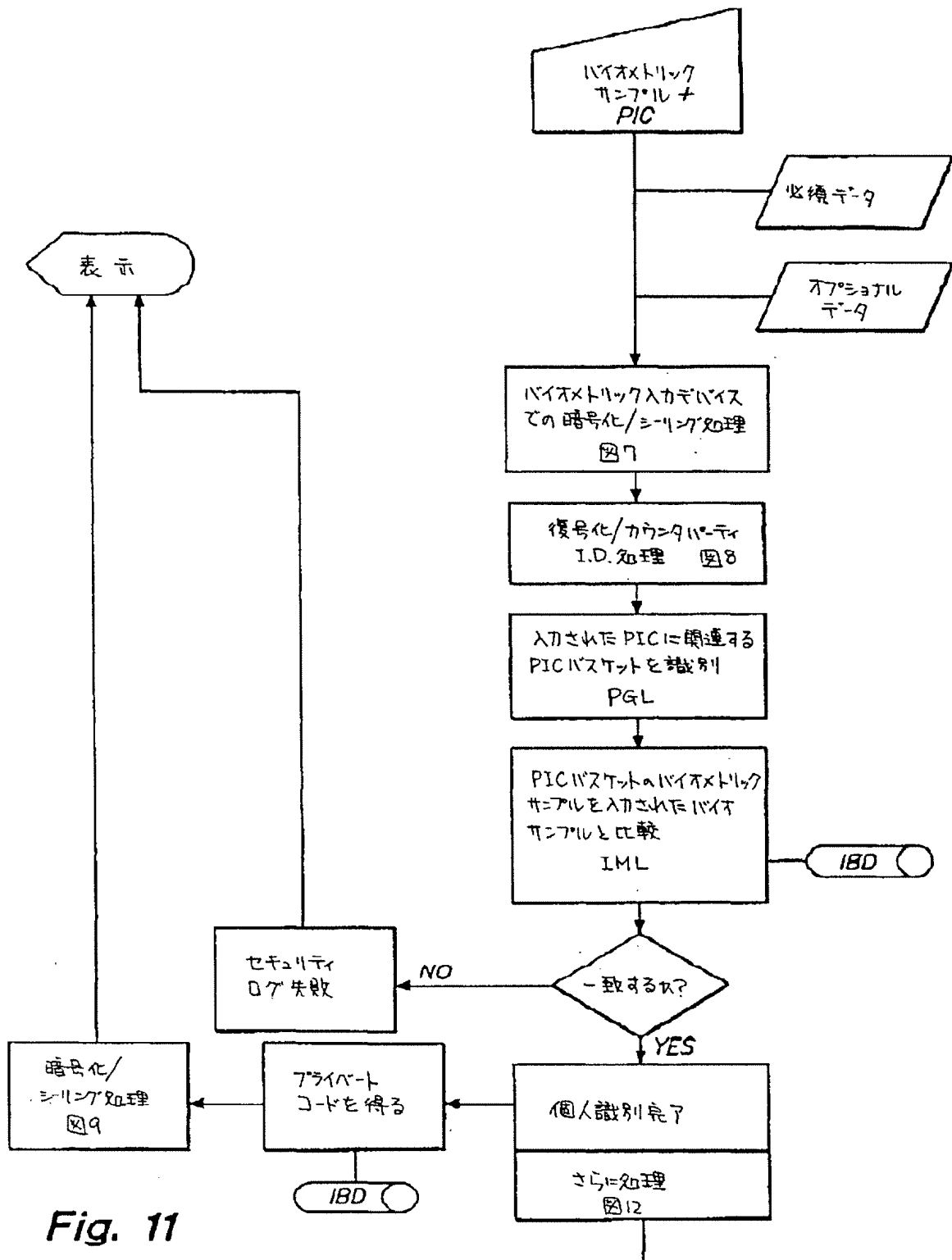


Fig. 11

【図12】

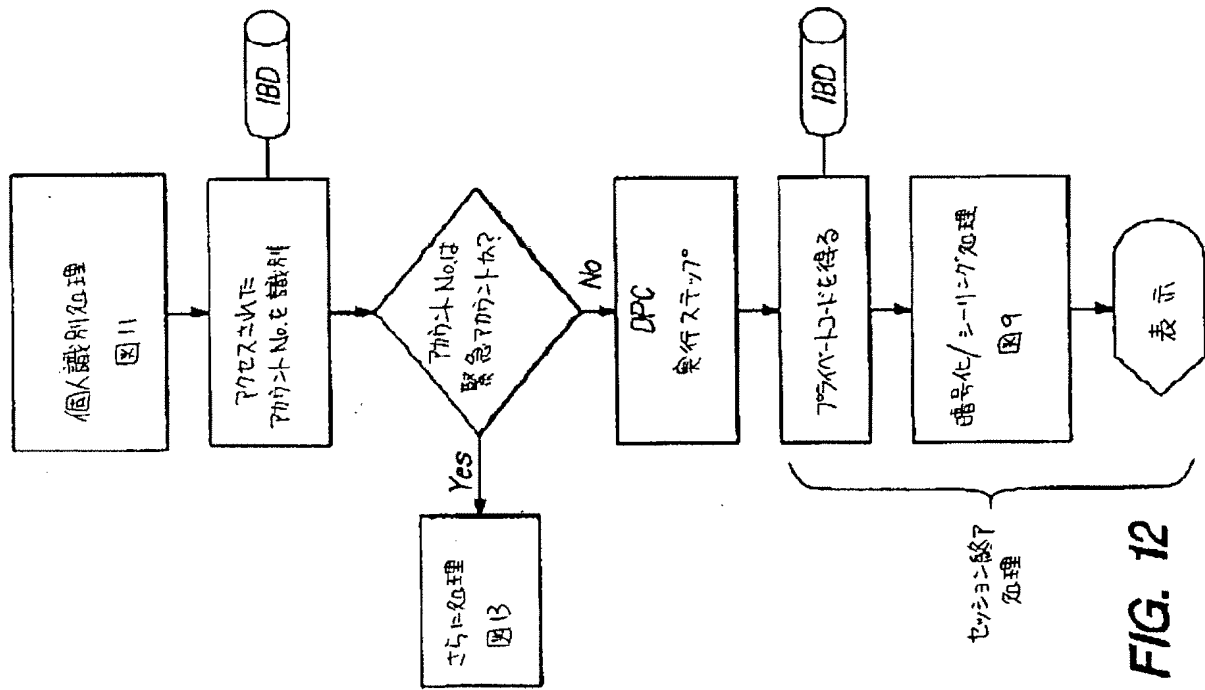


FIG. 12

【図13】

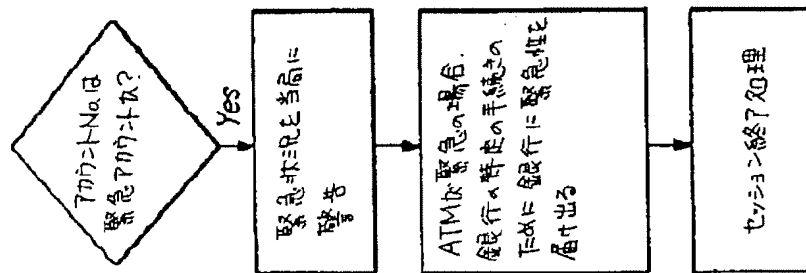


FIG. 13

【図14】

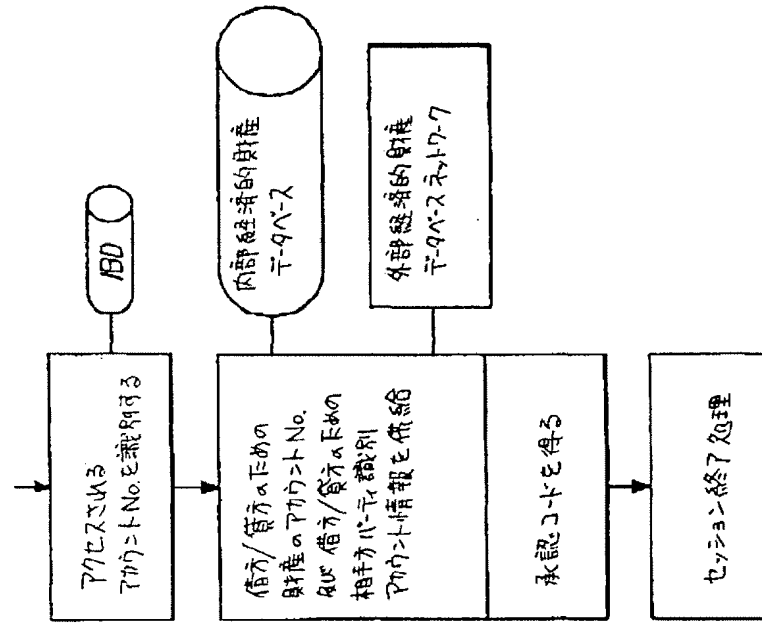


FIG. 14

【図15】

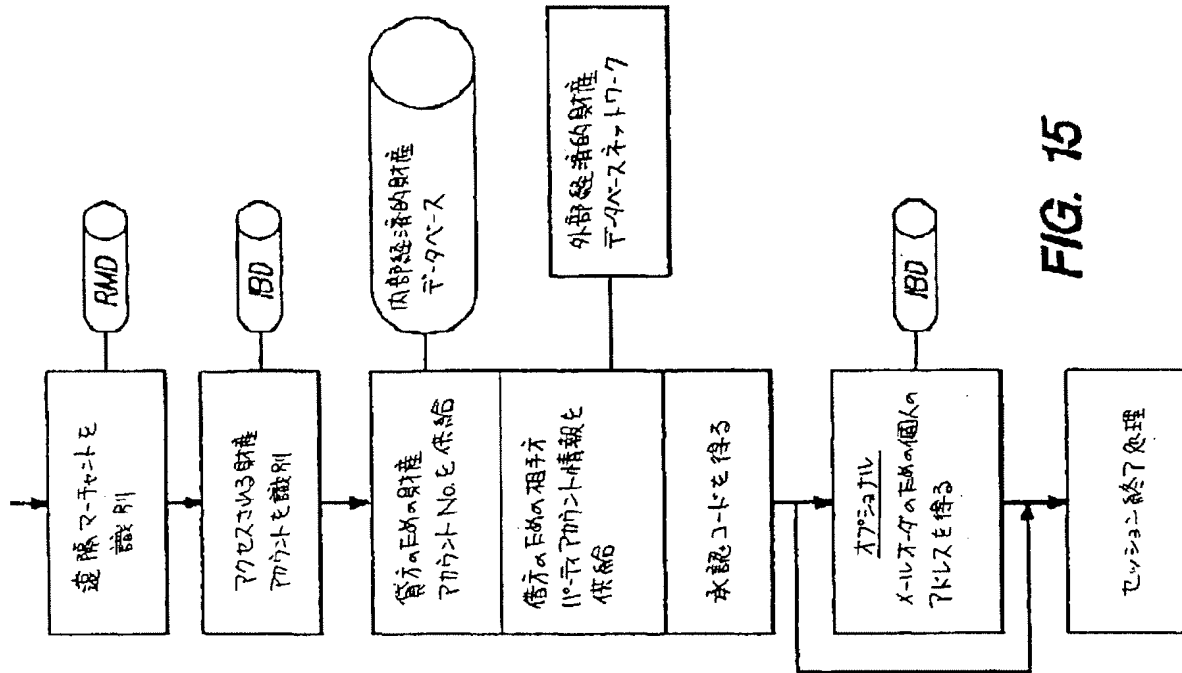
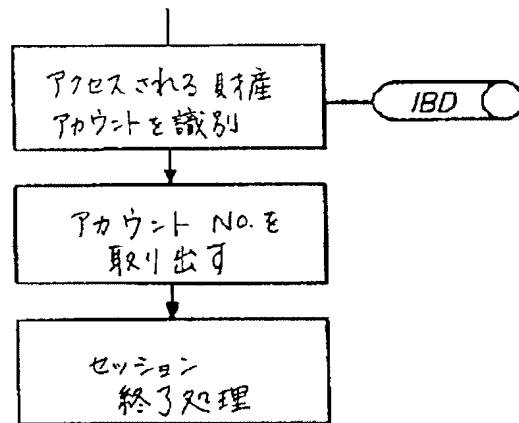


FIG. 15

【図16】

**FIG. 16**

【図 1 7】

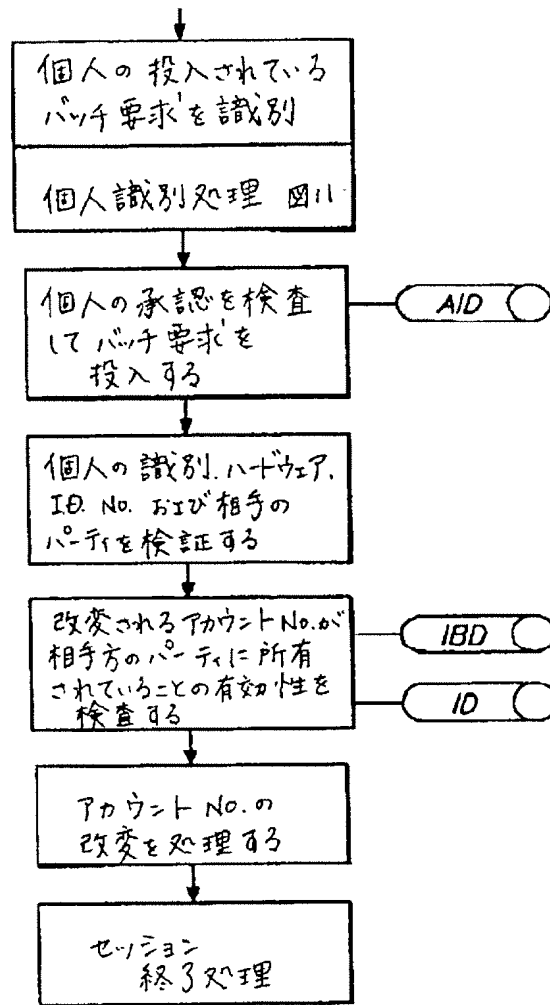


FIG. 17

【図 1 8】

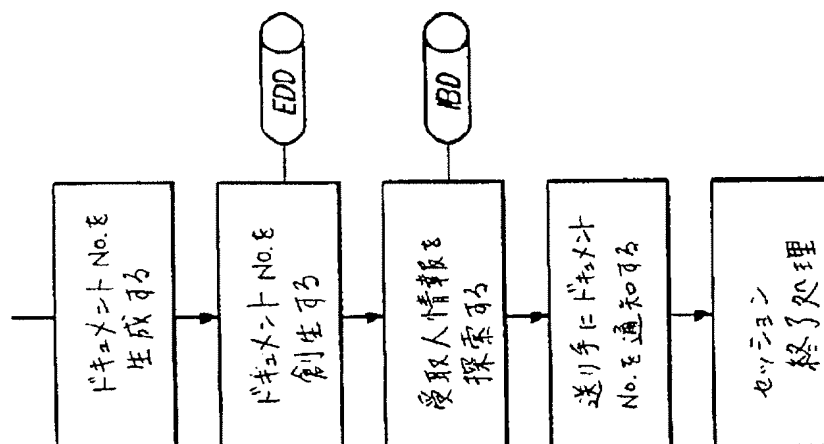


FIG. 18

【図19】

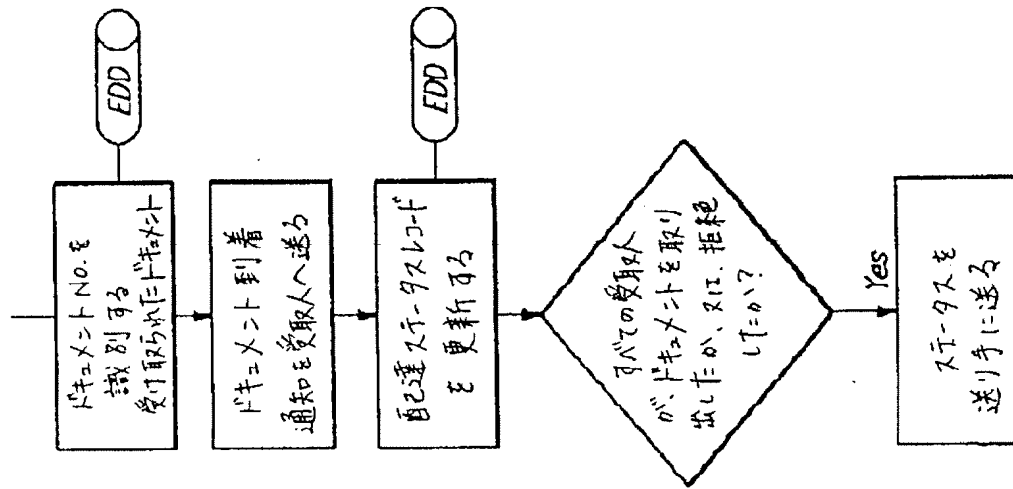


FIG. 19

【図20】

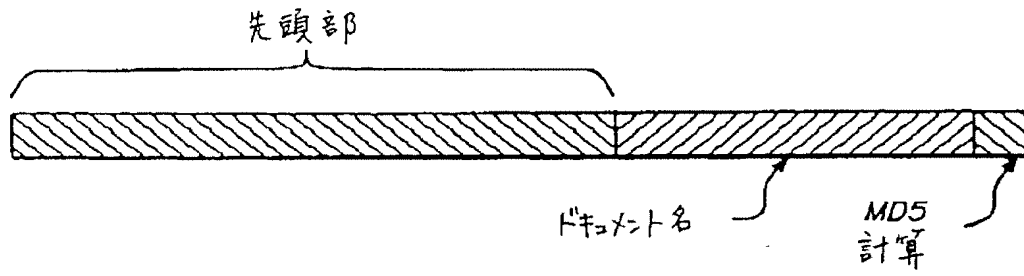


FIG. 20A

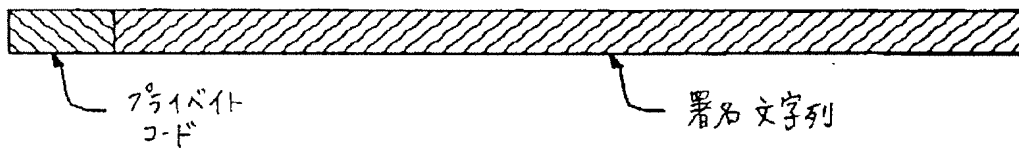


FIG. 20B

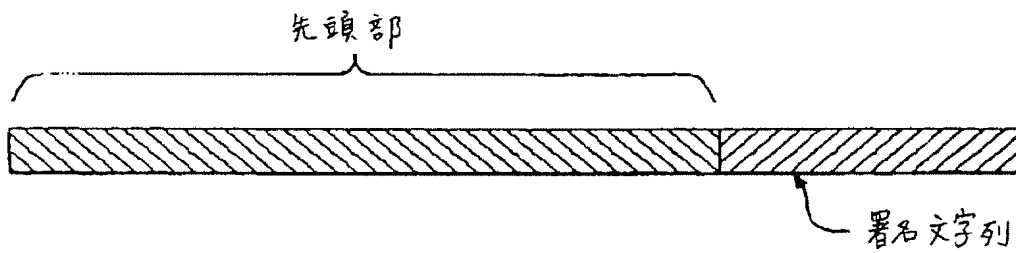


FIG. 20C

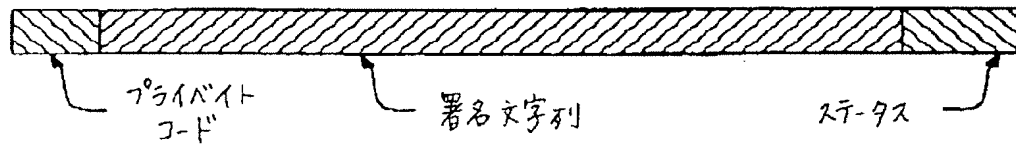


FIG. 20D

【図21】

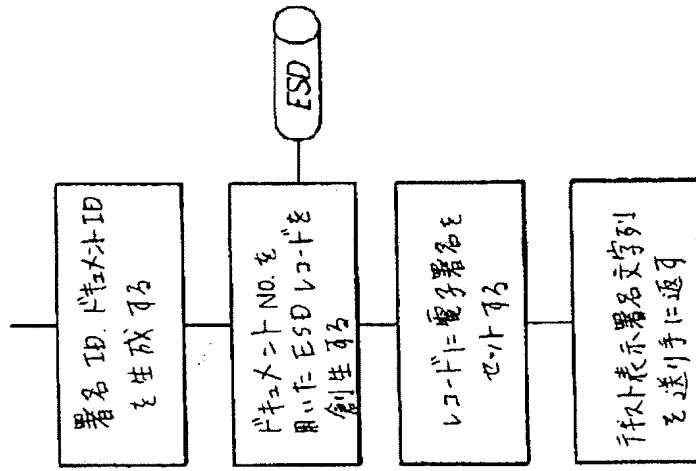


FIG. 21

【図22】

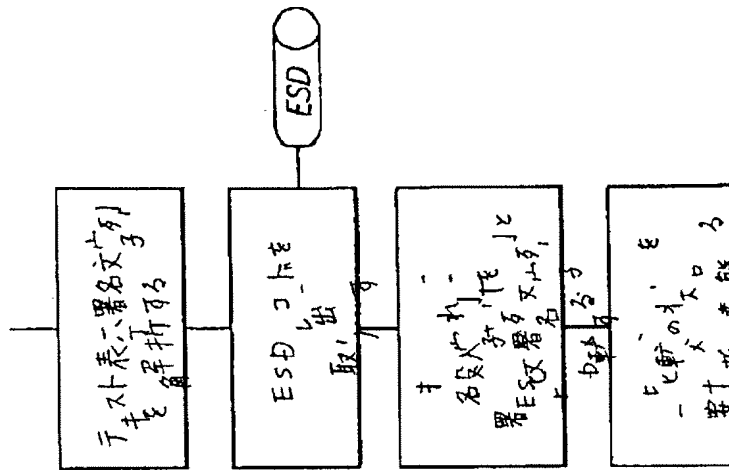


FIG. 22

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/07185

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : G06K 9/00

US CL : Please See Extra Sheet.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 902/1, 2, 3, 4, 5, 6, 22, 26, 27, 31, 32, 33; 340/825.34; 235/380; 382/115

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 5,229,764 (MATCHETT ET AL) 20 July 1993, see abstract, figure 1, column 1, lines 6-59, column 8, lines 19-25.	1-87
Y	US, A, 5,191,611 (LANG) 02 March 1993, column 16, line 27.	1-87

☐ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:	
A document defining the general state of the art which is not considered to be part of particular relevance	*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
E earlier document published on or after the international filing date	*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
O document referring to an oral disclosure, use, exhibition or other means	*Z* document member of the same patent family
P document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

03 JULY 1996

Date of mailing of the international search report

26 AUG 1996

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer
Leo Boudreau
LEO BOUDREAU

Telephone No. (703) 308-7595

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/07185

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

902/1, 2, 3, 4, 5, 6, 22, 26, 27, 31, 32, 33; 340/825.34; 235/380; 382/115

フロントページの続き

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, LS, MW, SD, SZ, UG), AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LT, LU, LV, MD, MG, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, UZ, VN

(72)発明者 リー, ジョナサン エイ.

アメリカ合衆国 カリフォルニア 94704,
バークレー, シャタック スクエア 46,
スイート 12